PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 3: G06F 15/30; G06K 5/00 — A1

(11) International Publication Number: WO 82/00213

(43) International Publication Date: 21 January 1982 (21.01.82)

(21) International Application Number: PCT/US81/00431

(22) International Filing Date: 2 April 1981 (02.04.81)

(31) Priority Application Number: 166,689

(32) Priority Date: 2 July 1980 (02.07.80)

(33) Priority Country: US

(71) Applicant; and
(72) Inventor: BENTON, William, M. [US/US]; Route 1, Box 191, Middleburg, VA 22117 (US).

(74) Agents: BECKER, Stephen, A. et al.; Lowe, King, Price & Becker, 2001 Jefferson Davis Highway, Arlington, VA 22202 (US).

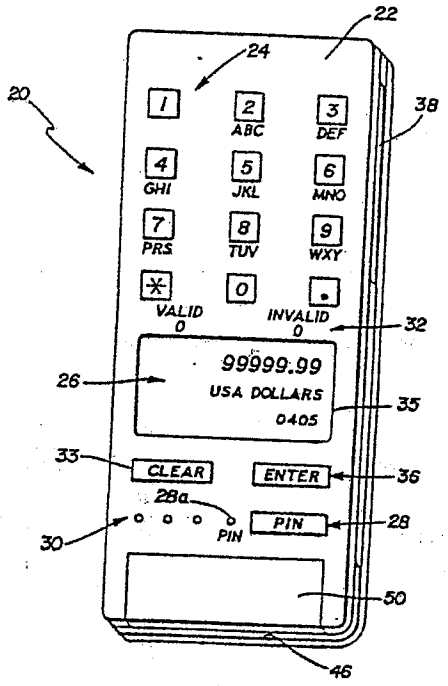
(81) Designated States: DE (European patent), FR (European patent), GB (European patent), JP, SE (European patent).

Published
With international search report

(54) Title: ELECTRONIC FUNDS TRANSFER AND VOUCHER ISSUE SYSTEM

(57) Abstract

In a system for transferring electronic funds data in lieu of cash between vendees and vendors associated with a sponsoring financial institution, each vendee is provided with an identification card (40) and a portable electronic device (20) to be presented to the vendor upon making a purchase. The electronic device contains a keyboard (24) for entering a vendee identification number as well as the purchase amount and a memory for storing a corresponding identification number, account balance and transaction amount. The portable electronic device contains a first inlet (38) for receiving an edge of the identification card. A magnetic head (44) reads data recorded on the card to turn the device on if the card corresponds to the particular device. A second inlet (46) within the device receives vouchers (48) prepared by the vendor reflecting the amount of the transaction. Manually operated printing rolls (54, 56) within the second inlet print a series of encoded bands on the voucher to verify the transaction if the vendee is satisfied with the purchase. If the vendee has keyboard entered the correct identification number and the account balance is large enough to support the purchase, the account balance stored in memory is debited by the purchase amount during a voucher printing cycle. The identification card and associated electronic device can be used in environments other than funds data transfer, e.g., access security.



JUMBO PATENT
DUE TO ITS EXCESSIVE LENGTH,
COMPLETE PATENT FURNISHED
UPON SPECIAL REQUEST ONLY.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**KP**	Democratic People's Republic of Korea
AU	Australia	**LI**	Liechtenstein
BR	Brazil	**LU**	Luxembourg
CF	Central African Republic	**MC**	Monaco
CG	Congo	**MG**	Madagascar
CH	Switzerland	**MW**	Malawi
CM	Cameroon	**NL**	Netherlands
DE	Germany, Federal Republic of	**NO**	Norway
DK	Denmark	**RO**	Romania
FI	Finland	**SE**	Sweden
FR	France	**SN**	Senegal
GA	Gabon	**SU**	Soviet Union
GB	United Kingdom	**TD**	Chad
HU	Hungary	**TG**	Togo
JP	Japan	**US**	United States of America

ELECTRONIC FUNDS TRANSFER AND VOUCHER ISSUE SYSTEM

TECHNICAL FIELD:

The present invention relates generally to access security systems, and more particularly, to an off-line electronic funds transfer system including a portable electronic device that stores account and identification data to authorize transactions and following transactions prints verification data onto vouchers.

BACKGROUND ART:

Several prior art systems of which I am aware have been provided for enabling electronic funds transfer to be made between vendees and vendors in lieu of cash. In Moreno 4,007,355, for example, cashless transactions are made using vendee and vendor credit cards through a special interface apparatus located at the vendor station. The cards themselves contain funds data storage capability. No voucher verifying the transaction is issued. Haker 4,032,931 discloses a keyboard assembly for transferring financial data between vendees and vendors. No cards are involved and funds data transfer is made during each transaction between the point of sale and a central computer.

Riccitelli 3,934,122, Schatz 4,001,550 and Dethloff 4,105,156 are examples of electronic funds transfer systems wherein credit cards containing memory devices store account balance and other information to be accessed during funds transfer transactions. There is no provision in these systems, however, for determining whether the transaction is authorized based upon vendee identification and account balance and no provision

BUREAU OMPI WIPO INTERNATIONAL

for issuing a voucher verifying the transaction.

Foudos 4,053,735 discloses a portable electronic device for issuing bank-assured checks wherein a credit amount is loaded into memory and transaction amounts successively debited from the credit balance. If the vendee keyboard enters correct vendee identification data, and the purchase amount, also keyboard entered, is less than the present account balance, the vendee is authorized to manually operate a check printer incorporated within the device for issuing the assured check.

In Link 3,651,310, a combination voucher and printer and credit card validator reads an identification number recorded on a credit card while imprinting the voucher and transmits this number to a memory. The credit card number is compared with a list of invalid credit card numbers to determine card validity.

In Nagata 4,197,986, a funds data transfer system is disclosed which is usable both on-line and off-line to authorize transactions. Account balance is stored on a credit card and electrically up-dated following each transaction. The card also controls issuance of a sales slip.

Goldman 3,982,103 discloses a credit card transaction verifier that reads account balance data as well as additional data magnetically recorded on a credit card. The recorded data are up-dated following each transaction. The verifier is adapted to operate either on-line or off-line.

In Case et al. 4,172,552, a credit card processing system includes a reader for reading data encoded in the magnetic stripe of a card.

BUREAU OMPI WIPO INTERNATIONAL

The same data are printed at the point of sale along the bottom of the vendor's bank sales slip. The card reader makes cuts in the bank copy to designate the transaction as a credit or charge transaction.

Two portable, microprocessor based calculator units for continuously storing account balance and transaction information are marketed by JS&A, 1 JS&A Plaza, Northbrook, Illinois 60062. The first device, known as "CORVUS CHECK-MASTER", keeps a running balance of expenditures against a total balance, alterable at any time by the user. The second device, known as "ELECTRONIC WALLET", contains two non-volatile memories for storing two difference balances that are selectively debited by entering transaction data at a keyboard. Neither device, however, is capable of verifying transactions or issuing validated transaction vouchers.

Accordingly, one object of the present invention is to provide a system for performing electronic funds transfer in lieu of cash transactions and for issuing transaction verifying vouchers in duplicate, wherein the copy is retained by the vendee for record keeping.

Another object is to provide such an electronic funds transfer system wherein the vouchers are printed with encoded data at the point of sale to verify completion of the transaction.

Another object is to provide such an electronic funds transfer system wherein each vendee is provided with a portable electronic device that verifies that the vendee is authorized to make a purchase transaction based upon proper entry of a vendee identification number as well as

BUREAU OMPI WIPO INTERNATIONAL

by verification of an adequate account balance.

A further object is to provide a new and improved electronic funds transfer device which stores account and transaction data and verifies vouchers or drafts by imprinting encoded data on the voucher or draft upon completion of each authorized transaction.

Another object is to provide a new and improved electronic funds transfer device that is portable and microprocessor based, is small enough to be carried in a wallet and has a width equal to the width of a standard credit card.

In commercial transactions, checks are mailed by the vendor to the issuing banks where the checks are posted, cancelled and returned by mail to the vendees. This process, known as check truncation, is expensive and costs of truncation increase with increasing postage rates. On ACH (Automatic Clearinghouse) banks are now permitted by the Government to issue a statement to customers summarizing previous transactions rather than returning cancelled checks. Customers, however, tend to prefer receiving cancelled checks for permanent record keeping.

An additional object of the invention, therefore, is to provide a system for transferring electronic funds data between vendees and vendors in lieu of cash, wherein a verified voucher is issued confirming each completed transaction, the voucher is forwarded by the vendor to the sponsoring institution and a copy of the voucher is retained by the vendee, thereby eliminating conventional check truncation.

BUREAU OMPI WIPO INTERNATIONAL

DISCLOSURE OF INVENTION:

In a system for providing electronic funds transfer in lieu of cash between vendees and vendors under the sponsorship by an authorized financial institution, each vendee carries an identification card and pocket-sized, microprocessor based electronic device, or verificatory, that stores account and transaction data and imprints encoded data on vouchers or drafts presented by vendors for verification during transactions. Each verificatory includes a keyboard for entering identification and transaction data and a readout for displaying the account balance and amount of a current transaction. In addition, the verificatory includes sequence indicator lamps for requesting input data and displaying valid and invalid entries.

A first inlet at one side of the verificatory is adapted to receive an edge of the identification card having institution issued indicia recorded thereon. An electromagnetic head within the first inlet reads the card data for comparison with prerecorded corresponding data. If there is a match between the card data and prerecorded data, the keyboard is enabled.

A second inlet at one end of the verificatory is adapted to receive vouchers or drafts supplied by the vendor for verification following authorization and completion of a requested purchase transaction. A set of printing rolls within the second inlet prints encoded verification bands on the draft or voucher to verify completion of the transaction. The set of rolls comprises a pair of rolls normally separated from each other at the inlet to permit the voucher or draft to be inserted between them. The upper roll contains a series of bands having

BUREAU OMPI WIPO INTERNATIONAL

widths and interband spacings corresponding to data identifying the vendee account. To complete a purchase transaction, the vendee manually moves the identification band roller into contact with the voucher to impart thereto the identification band verification markings.

In operation, the vendee presents his card and verificatory at the point of sale, and enables the device by inserting the identification card into the first inlet in the verificatory. The vendee then removes the identification card from the verificatory and hands the card to the vendor for preparation of a voucher using a conventional credit card imprinter of a type supplied, for example, by Addressograph-Multigraph, International. To make a payment, the vendee keyboard enters the amount of the transaction and presses an ENTER key. The transaction amount is displayed in the readout. The vendee is then instructed by the verificatory via the sequence indicator to keyboard enter the personal identification number. The verificatory now automatically compares the keyboard entered identification number with a prerecorded identification number in ROM and compares the keyboard entered transaction amount with the account balance stored in RAM. As a safeguard, the device is programmed to respond to entry of an incorrect personal identification number. If the keyboard entered personal identification number does not match the stored personal identification number, the vendee is required to make two successive entries of the correct personal identification number. This procedure reduces the possibility of use of the device

BUREAU OMPI WIPO INTERNATIONAL

by an unauthorized vendee attempting to enter identification data based on guess work.

Assuming that the keyboard entered identification number matches the stored identification number and that the keyboard entered transaction amount is less than or equal to the stored account balance, the sequence indicator will indicate to the vendee and vendor that the transaction is authorized. The voucher, prepared by the vendor to indicate the transaction amount, is inserted into the second inlet of the verificatory between the printing rolls. The banded printing roll is now pressed against the voucher and the voucher withdrawn from the inlet to make the verification markings. As the verification markings are being printed onto the voucher, the amount of the requested transaction is subtracted from the account balance stored in RAM and the result is stored. The account balance and amount of last transaction are displayed on demand using, respectively, the "0" and "*" keys.

The identification card and associated verificatory can be used in systems other than funds data transfer, e.g., access security. Access to a restricted area is given only to authorized personnel by inserting a security card held by the candidate requesting entry into the verificatory and having the candidate keyboard enter his personal identification number. If entry is authorized the verificatory signals the authorization and prints an approval voucher. The voucher is later machine read to provide a traffic summary.

Still other objects and advantages of the present invention will become readily apparent

BUREAU OMPI WIPO INTERNATIONAL

to those skilled in this art from the following detailed description, wherein I have shown and described only the preferred embodiment of the invention, simply by way of illustration of the best mode contemplated by me of carrying out my invention. As will be realized, the invention is capable of other and different embodiments, and its several details are capable of modifications in various obvious respects, all without departing from the invention. Accordingly, the drawings and description are to be regarded as illustrative in nature, and not as restrictive.

BRIEF DESCRIPTION OF DRAWINGS:

Figure 1 is a perspective view of a microprocessor based, electronic funds transfer device in accordance with the invention;

Figure 2 is a back view of the device in Figure 1 showing a memory access terminal and back plate lock;

Figure 3 is a side view of the device in Figure 1 showing the first inlet for receiving an encoded portion of an identification card;

Figure 4 is an end view of the device in Figure 1 showing the second inlet for receiving vouchers for verification;

Figure 5 is a top view of an identification card used in the invention;

Figure 6 is a top view of a voucher used in the invention;

Figure 7 is a cross sectional view of the device in Figure 1 exposing the card reader within the first inlet;

Figure 8 is a cross sectional view of the device in Figure 1 showing details of the printing rolls;

BUREAU OMPI WIPO INTERNATIONAL

Figure 9 is a perspective view of the banded printing roll shown in Figure 8;

Figure 10 is a block diagram of circuitry constituting the device in Figure 1; and

Figures 11a-11d are a block diagram representing firmware for programming the microprocessor shown in Figure 1.

BEST MODE FOR CARRYING OUT THE INVENTION:

Referring to Figures 1-4, an electronic device 20, referred to hereinafter as verificatory, is used together with an identification card 40 (Figure 5) to determine whether an individual presenting the card is authorized to receive a privilege issued by a sponsoring institution, e.g., to gain access to a security area or to complete a funds data transaction, and upon authorization, to issue an encoded verification document. Although the present invention is applicable in many limited access environments, the present description shall be directed by way of example to electronic funds data transfer.

Verificatory 20 includes an impact resistant plastic housing 22 carrying a push button keyboard 24, a first display 26 for displaying account and transaction data and a second display 30 for displaying the operating sequence of the verificatory. Housing 24 also carries a third display 32 indicating whether a requested transaction is valid or invalid, a key 33 for clearing keyboard entered data, a key 28 for enabling the verificatory to accept a vendee personal identification number (PIN) and an ENTER key 36 for causing the verificatory to accept keyboard entered data. A first inlet 38 at one side of the housing 22 receives

BUREAU CMPI WIPO INTERNATIONAL

an edge portion of the identification card 40 for reading data magnetically encoded on stripe 42 (see Figure 5). The magnetic data are read by an electromagnetic head 44 located within the housing 22 adjacent inlet 38, as shown in Figure 7. A second inlet 46 positioned at one end of the housing 22 is adapted to receive vendor issued transaction vouchers, such as voucher 48 shown in Figure 6. Adjacent the inlet 46 of the housing 22 is a manually depressable bar 50 that causes encoded verification data in the form of bands 51 (see Figure 6) to be printed on an end portion of the voucher 48. A gate 57 suspended from print bar 50 at pivot 59 and spring biased in a closed position encloses the inlet 46 in the absence of a voucher 48. The gate 57 provides two functions; it seals the inlet from ingress of dust and makes it impossible to initiate a print cycle by depressing bar 50 in the absence of a voucher 48.

Referring to Figure 8, a pair of printing rolls 54 and 56 are rotatably supported on bar 50 and lower housing portion 53 within recesses 58 and 60, respectively. The bar 50 in turn is supported on upper housing portion 55 (Figure 3) by pins 62 that ride within elongated slots 64 formed in the housing. The bar 50 is biased by springs (not shown) into the position shown in Figure 8 wherein roll 54 is separated from roll 56 by a distance substantially larger than the thickness of a voucher 48. The upper roll 54, shown in detail in Figure 9, is formed with surface bands 66 having widths and interband spacings corresponding to data identifying the vendee. The band portions 66 of the upper roll 54 are

BUREAU OMPI WIPO INTERNATIONAL

permanently impregnated with graphite or other printing medium. Alternatively, voucher 48 may be provided with a carbon paper layer.

The voucher 48, when inserted into inlet 46, rests on lower roll 56 as well as on a switch operator 68 that is in contact with the lower surface of voucher 48. A normally open electrical switch 69 is closed by downward indexing of the operator 68 by print bar 50. The operator 68 extends slightly above the top of lower roll 56. Thus, when bar 50 is manually depressed by the vendee with a voucher 48 in position within inlet 46, as shown in Figure 8, the operator 68 is urged downwardly closing the electrical switch 69 while printing roll 54 is pressed into printing position on the upper surface of the voucher. The closing of electrical switch 69 signals to the verificatory 20 that a printing operation is under way. With the print bar 50 still depressed, the vendee withdraws the voucher 48 from the housing 22 to cause the upper surface of the voucher to become imprinted with the identification bands 51 (Figure 6).

Referring now to Figure 10, electronic circuitry 70 within housing 22 includes a microprocessor 72, such as a Motorola Model 6800, 8-bit microprocessor interfaced with an ROM 74 and a RAM 76. The RAM 76 may be a Motorola Model 5101 integrated circuit; ROM 74 may be a Motorola Model MC65830A integrated circuit. It is to be understood, however, that other microprocessors or memories could be used providing quiescent current drain is low. Low quiescent current drain is important since microprocessor 72 and RAM 76 are always energized. The RAM must remain energized since it is a volatile memory; the

BUREAU OMPI WIPO INTERNATIONAL

microprocessor must remain energized to process card read data (there is no on/off key).

Microprocessor 72 is also interfaced to receive data manually entered by keyboard 24. A switch 78 between keyboard 24 and microprocessor 72, controlled by card reader 44, inhibits the output of the keyboard 24 unless the data magnetically encoded in stripe 42 of identification card 40 are identical to corresponding data stored in ROM 74. Thus, switch 78, which is normally open, is closed to enable entry of keyboard data to microprocessor 72 only if card 40 inserted within inlet 48 is the card that is issued for use with the particular verificatory 20; otherwise, the device is disabled. The verificatory 20 is thus, in a sense, "turned on" by card 40; there is no on/off key within keyboard 24 and, as aforementioned, the electronic circuitry within the verificatory 20 is never deenergized. Alternatively, the circuitry 70, except for RAM 76, may be normally de-energized to conserve battery power, and energized only when card 40 is inserted within inlet 38 in response to closure of a microswitch (not shown) within the inlet.

The microprocessor 72 is also interfaced with print bar 50 through switch 69. The switch 69, as mentioned above, is normally open and is closed in response to depression of switch operator 68 during a manual printing cycle.

Also interfaced with microprocessor 72 are account and transaction numerical display 26 as well as sequence lamps 30, 32. The data supplied to display 26 and lamps 30, 32 by microprocessor 72 are obtained from ROM 74 and RAM 76. The RAM 76 includes a pair of accumulators

BUREAU OMPI WIPO INTERNATIONAL

A and B for temporarily storing keyboard entered transaction and personal identification data as well as for storing account balance data. Data to be displayed by display 26 as well as by lamps 30, 32 are supplied to the display and lamps by accumulators A and B. These accumulators A and B also provide temporary storage of data during arithmetic manipulation by microprocessor 72 in a conventional manner.

Microprocessor 72 is also interfaced with a data generator 80 located at the authorized institution for issuing credit to the vendee by supplying to the microprocessor and RAM 76 an initial account balance which may reflect an amount maintained by the vendee on deposit with the institution or may represent an amount greater than the deposit reflecting a credit advance. The output of generator 80 is supplied to microprocessor 72 through external terminals 84 on the rear of housing 22 behind backing plate 88, as shown in Figure 2. Backing plate 88 is provided with an access slot 86 for receiving a key held by the sponsoring financial institution. The access slot 86 enables the sponsoring institution to remove back plate 88 to load RAM 76 with initial or supplemental funds, to change batteries 90 (Figure 10), or to inspect or service the circuitry 70.

Microprocessor 72 is programmed by firmware in ROM 74 to operate in either a payment mode, a status request mode or a transaction verification mode. The payment mode enables the vendee to make purchases from a vendor using electronic funds data transfer in lieu of cash. In the status request mode, the verificatory 20 displays

BUREAU OMPI WIPO INTERNATIONAL

the account balance. In the verification mode, the amount of the last transaction is displayed. In all three modes, the verificatory 20 is rendered operative only if the identification card 40 is an authorized one and if the vendee keyboard enters the correct personal identification number.

In the payment mode, characterized by the making of a purchase of goods or services by a vendee from a vendor, both of whom are members of a sponsoring institution, the vendee presents funds transfer device money and card 40 at the point of sale. The vendee inserts card 40 into inlet 38. Data magnetically prerecorded on the card 40 is read by head 44. If the card 40 is not the proper card corresponding to that particular verificatory 20, the device 20 will remain disabled; there will be no response. If the card is verified as being a proper card corresponding to that verificatory 20, on the other hand, the "P" lamp of sequence display 30 will light indicating that payment data are being requested. The amount of the payment transaction is now keyboard entered and that amount is displayed in readout 26 for visual verification. ENTER key 36 is now depressed to cause the transaction amount data to be stored in memory 76; the display 26 is reset. PIN display 28a is energized to indicate that entry of the personal identification number is requested. Following depression of PIN key 28, the personal identification number is keyboard entered by the vendee, followed by depression of ENTER key 36. The personal identification number is not displayed. Only if the keyboard entered personal identification number matches the institution issued personal identification number stored in ROM 64, the PIN indicator 28a will

BUREAU OMPI WIPO INTERNATIONAL

turn off. If the keyboard entered personal identification number is incorrect, as another level of security, the verificatory 20 will require the vendee to keyboard enter the personal identification number correctly twice in succession. The keyboard entered transaction amount is now compared with the account balance. If the account balance is greater than or equal to the transaction amount, the VALID lamp of indicator 32 will turn on; otherwise, the INVALID lamp turns on.

A voucher 48 (Figure 6) supplied by the vendor and containing the summary of the transaction is positioned within inlet 46 for printing of verification bands 51. With the voucher properly aligned, and the vendor having witnessed that the VALID lamp is energized, the vendee depresses the print bar 50 and withdraws the voucher 48, thereby imprinting verification bands 51 on the surface of the voucher. The VALID lamp 32 is now deenergized and the transaction amount displayed in readout 26 is replaced with the word PAID. The PAID display remains visible for approximately six seconds or other predetermined time interval. The transaction amount is now subtracted from the account balance and the new balance is stored in RAM 76. The amount of the transaction is stored in a separate portion of memory to be accessed for later verification if requested. The voucher 48 is signed by the vendee; the vendee keeps the original and a copy is given to the vendor. The copy is forwarded by the vendor to the sponsoring financial institution where the vendee's account is debited. Since the original copy of the voucher has been cancelled by imprinting thereon bands 51, the original voucher is cancelled; there

BUREAU OMPI WIPO INTERNATIONAL

is no need for separate truncation by the sponsoring institution.

To make a status request wherein the account balance is displayed in readout 26 or to make a transaction verification wherein the amount of the immediately previous transaction is displayed, the identification card 40 is positioned in inlet 38 of the housing 22. If the identification card 40 correctly corresponds to the verificatory 20, e.g., the card and verificatory have identical account numbers (the last four numbers of the account may be printed on the verificatory as shown in Figure 1 at 35), the P lamp of sequence display 30 is energized. The * key is depressed to indicate to device 20 that a status request is being made. The ENTER key 36 is now depressed and in response, the PIN sequence indicator 28a is energized. The personal identification number is keyboard entered by the vendee. Assuming the keyboard entered personal identification number matches the personal identification number stored in ROM 74, the S lamp is energized and the P lamp is deenergized. If the account status is to be displayed, the "0" key and ENTER key are successively depressed. If verification of the immediately previous transaction is to be displayed, however, the * key and ENTER key 26 are successively depressed. If the personal identification number entered by the vendee at keyboard 24 does not match the personal identification number stored in ROM 74, PIN sequence indicator 28a will not be deenergized and no information will be displayed or transaction approved unless the correct personal identification number is keyboard entered by the vendee correctly

BUREAU OMPI WIPO INTERNATIONAL

twice in succession.

The contents of RAM 76 and ROM 74 are as follows:

RAM Locations

0100 - Cash which is available in account.

0101 - Amount to be paid out.

0102 - Amount of last transaction.

0103 - Personal identification number (PIN).

0104 - Control number furnished by banking institution.

0105 - Record of wrong PIN number submitted by operator.

0106 - Area used by processor to determine if a payment request has been initiated.

0107 - Area used by processor to determine if a status request has been initiated.

0108 - Card identification number.

ROM Locations

0200 - PIN number.

0201 - Control number.

0202 - Contains the encoded value for displaying the "PAY" indicator.

0203 - Contains the encoded value for displaying the "PIN" indicator.

0204 - Contains the encoded value for displaying the "STATUS" indicator.

0205 - Contains the encoded value for displaying the "INVALID" indicator.

0206 - Contains the encoded value for displaying the "VALID" indicator.

0207 - Contains the encoded value to cause the display to exhibit the word "PAID".

0208 - Contains card identification number.

0209 - Contains logarithm of card identification number.

Microprocessor 72 is programmed to perform the sequence of operations described above.

BUREAU OMPI WIPO INTERNATIONAL

An examplary program in accordance with the preferred embodiment is illustrated in Figures 11a-11d. Each programming step shown in those Figures is conventional and known by persons of ordinary skill in the microprocessor programming art.

Referring first to Figure 11a, the vendee first inserts identification card 40 into inlet 38 of the housing 22 to cause the magnetic stripe 42 to be read by magnetic head 44 (see sequence block 100). The identification number read from stripe 42 is stored at location 0108 in RAM 76 (block 102). The card identification number is now transferred from memory location 0108 to accumulator A (block 104).

Accumulator B is loaded with the card number permanently stored at location 0208 of ROM 74 (block 106). The card read number in accumulator A is now compared with the prerecorded card number in accumulator A (block 108). If the two numbers are not equal to each other (block 109), indicating that the inserted identification card is not the one issued with the particular verificatory 20, the memory location 0108 containing the card read data is cleared (block 110) and the program is stopped (block 112).

If the two identification numbers stored in accumulators A and B are equal to each other, however, the subroutine from ROM location 0209 is operated to display a number stored at ROM location 0209 (block 111) which may be the logarithm of the card identification number. This displayed number is viewed by the vendor and written onto voucher 48 to verify that the vendor has actually viewed the verificatory 20 for additional security. The subroutine from ROM location 0202 is now

BUREAU OMPI WIPO INTERNATIONAL

executed to energize the pay indicator lamp P of readout 30 (block 114). The vendee keyboard enters the transaction amount followed by depression of the ENTER key (block 116) and that amount is stored in RAM 76 at location 0101 (block 118). The display subroutine stored in ROM location 0203 is operated to energize the "PIN" indicator lamp in readout 30 (block 120). The vendee now keyboard enters the PIN number (block 122) followed by depression of the ENTER key and that number is stored in RAM 76 at location 0103 (step 124). If the present transaction is a pay request (step 126), i.e., the vendee has made an entry in accordance with block 116, a logical one signal is stored in RAM 76 at location 0106 as a flag (block 128). If no transaction amount has been keyboard entered in accordance with block 116, the device 20 is programmed to enter a status request or transaction verification mode. In that mode, a display subroutine from ROM 74 at location 0204 is operated to energize the status indicator S in readout 30 (block 132). If an account status check is required, the vendee makes a status request by operating the "0" and ENTER keys in succession (block 134). If a status request is made (block 136), a logic one flag signal is stored in RAM 76 at location 0107 and the program branches to point A in Figure 11b (block 140). Otherwise, the program branches directly to point A (block 142) without setting the flag bit at RAM location 0107.

Referring now to Figure 11b, the personal identification number stored at RAM location 0103 is loaded into accumulator A (block 144). The personal identification number prerecorded at ROM location 0200 is loaded into accumulator

BUREAU OMPI WIPO INTERNATIONAL

B (block 146). The contents of the two accumulators are compared with each other (block 148) to determine whether there is a match (block 150). If the two PIN numbers are unequal to each other, indicating that the keyboard entered number is improper, accumulator A is cleared (block 152) and incremented (block 154). The content of accumulator A, which has a decimal one value, is stored at RAM location 0105 (block 156). RAM locations 101, 103, 106 and 107 are now cleared (block 158) and subroutine 0205 (block 160) is operated to energize the INVALID lamp on readout 32 before stopping the program (block 162). It should be noted at this point that RAM location 0105 indicates that the PIN number has been improperly keyboard entered one time.

If the keyboard entered PIN number matches the PIN number stored in ROM 74, the flag bit stored in RAM location 0105 indicating that the personal identification number was previously incorrectly keyboard entered is loaded into accumulator A (block 164). Accumulator B is now cleared (block 166) and the two accumulators compared (block 168). Block 168 determines whether the content of accumulator B has a value of logic zero indicating that an improper PIN has not been previously entered or a value of logic one indicating that an improper PIN has been previously entered. If the contents of accumulators A and B do not match, i.e., the content of accumulator A has a value of one (block 170), the content of accumulator B is stored at RAM location 105, i.e., RAM location 105 is reset (block 172). RAM locations 101, 103, 106 and 107 are reset (block 174) and the display subroutine at ROM

BUREAU CMPI WIPO INTERNATIONAL

location 0205 is operated to energize the INVALID lamp on housing 22 (block 176) before stopping the program (block 178).

If, on the other hand, the contents of accumulators A and B are equal to each other in accordance with block 170, the program tests the integrity of RAM 76 by loading a control word stored at RAM location 104 into accumulator A (step 180) and then loading a corresponding control word stored at ROM location 0201 into accumulator B (block 182). Contents of accumulators A and B are compared with each other (block 184). If the contents of the two accumulators are unequal, indicating that RAM 76 has been tampered with, altered or otherwise has failed, display subroutine 0205 is executed to energize the INVALID indicator (block 188), RAM locations 0101, 0103, 0106 and 0107 are cleared (block 190) and the program is stopped (block 192). If the contents of the two accumulators A and B are equal to each other, however, the integrity of RAM 76 is considered to have been affirmed, and the flag bit stored at RAM location 106 indicating that a payment request has been initiated is loaded in accumulator A (block 194). Accumulator B is cleared (block 196) and the contents of accumulators A and B are compared with each other (block 198). This sequence merely tests the content of RAM location 106 to determine whether location 106 contains the flag bit. If the contents of accumulators A and B are not equal to each other, indicating that there is a flag bit at RAM location 106 identifying a pay request, the transaction amount stored at RAM location 0101 is loaded into accumulator B (block 200).

BUREAU OMPI WIPO INTERNATIONAL

The program now branches to a pay routine (block 202) at point C in the program (Figure 11d). If the contents of accumulators A and B are not equal to each other, however, indicating that a payment request has not been initiated, the content of RAM location 107 which identifies whether a status request has been initiated in accordance with block 134 is loaded into accumulator A (block 204). The contents of accumulators A and B (accumulator B has been previously cleared in accordance with block 196) are compared (block 206) to determine whether accumulator A contains a flag bit indicating a status request. If the contents of the two accumulators A and B are not equal to each other, indicating that there is a flag bit in accumulator A and that a status request has been made (block 208), the program branches to point D (Figure 11d) to execute a status check routine. If the contents of accumulators A and B are equal to each other, however, there is no flag bit stored at RAM location 0107 and a transaction verification request is implied. Accordingly, the amount of the last transaction at RAM location 0102 is loaded into accumulator A (block 212) for display (block 214) at readout 26. Accumulator A in RAM locations 101, 103, 106 and 107 are now cleared (step 216) and the program is stopped (block 218).

Referring to Figure 11d, if a status request has been made as determined in accordance with block 208, the account balance stored at RAM location 0100 is loaded into accumulator A (block 220) to be displayed (block 222) at readout 26. Accumulators A and B as well as RAM locations 101, 103, 106 and 107 are cleared (block 224)

BUREAU OMPI WIPO INTERNATIONAL

and the program is stopped (block 226).

Assuming that a pay request has been made in accordance with block 126, the account balance stored at RAM location 0100 is loaded into accumulator A (step 228). The contents of accumulators A and B (accumulator B contains the amount of the purchase transaction obtained from RAM location 0101 in accordance with block 200) are compared (block 230). If the content of accumulator A is less than the content of accumulator B (block 232) indicating that there are insufficient funds to support the payment transaction, subroutine 0205 (block 234) is executed to energize the INVALID lamp and the program is stopped (block 236). If the content of accumulator A is greater than or equal to the content of accumulator B, on the other hand, indicating that there are sufficient funds to support the requested payment transaction, subroutine 0206 stored in RAM is executed to energize the VALID lamp (block 238).

The content of accumulator B identifying the transaction amount is displayed at readout 26 (block 240) and the program is interrupted (block 242). The program interruption is removed in response to closure of switch 69 (Figure 10) during a transaction verification printing operation using print bar 50 (block 244). The amount of the transaction stored in accumulator A is subtracted from the account balance stored in accumulator B (block 246) and the resultant balance is stored at RAM location 0100 (block 248). The content of accumulator B (transaction amount) is stored at RAM location 0102 (block 250). The display subroutine at ROM location 0207 is now executed to display the word PAID on the alphanumeric

BUREAU OMPI WIPO INTERNATIONAL

display of readout 26 (block 252). Accumulators A and B as well as RAM location 101, 103, 106 and 107 are cleared (block 252) and the program is stopped (block 254).

In this disclosure there is shown and described only the preferred embodiment of the invention, but, as aforementioned, it is to be understood that the invention is capable of use in various other combinations and environments and is capable of changes or modifications within the scope of the inventive concept as expressed herein. For example, the verificatory 20 in addition to financial security is useful and beneficial in personel security to authorize entry to a restricted area or to provide personnel identification. The verificatory 20 sans printer may, for example, be carried by a person seeking entry to a restricted area and an imprinter maintained by a guard. A prearranged pass code number is displayed to the guard. The pass code display is displayed in the device for next guard who may require still another number. The imprinted document becomes a record of entry. A copy becomes part of the badge to be carried by the authorized entrant. The verificatory 20 will gradually run out of authorization numbers which will require reloading. This is another security feature as high security would require limited number of authorized entrants. In another mode, the verificatory and imprinter are both maintained by the guard and the authorized person has the card and knows the PIN number. A different coded magnetic card would operate the verificatory in highly restricted areas and would require knowledge of a different PIN number. In still

BUREAU OMPI WIPO INTERNATIONAL

another mode, armies, especially armies on foreign soil, could receive pay or portion via loading of the device and still use the device in its simple form for security entry and identification. The service serial number of the individual would be programmed in the verificatory as the personal identification number. Of particular significance, a single verificatory 20 may be used in the financial and access security environments as well as other environments without modification.

The system described above, while ideal in an electronic funds transfer (EFT) environment will also guarantee standard checks by imprinting verification bands on the back of the check while debiting the account balance stored in the verificatory 20.

BUREAU OMPI WIPO INTERNATIONAL

CLAIMS:

1. An apparatus for transferring funds data in lieu of cash, comprising a portable unit to be carried by a vendee, said portable unit including a keyboard for manually entering transaction and identification data, terminal means accessible only by an authorized institution for receiving an initial funds balance; means coupled to said terminal means for storing a funds balance, means responsive to said keyboard for storing a requested transaction amount, means for storing vendee identification data issued by said institution, means responsive to said keyboard for storing vendee entered identification data, means for comparing said stored identification data with said keyboard entered identification data and for generating a first signal in response to a positive comparison, means for comparing said stored funds balance with said requested transaction amount and for generating a second signal if said funds balance is at least as large as said requested transaction amount, an inlet for receiving a voucher issued by a vendor, manually actuated printing roll means within said inlet for printing encoded identification data onto said voucher to verify the transaction, means for maintaining said printing roll means normally out of contact with said voucher within said inlet, means for manually moving said printing roll means into contact with said voucher, means responsive to said manual means and to said first and second signals for updating said stored funds balance by said requested transaction amounnt, and display means for displaying said stored funds balance

BUREAU OMPI WIPO INTERNATIONAL

and said requested transaction amount.

2. A system for transferring funds data between a vendee and vendor in lieu of cash, comprising a fixed unit located at a sponsoring institution for generating credit data to be provided to member vendees; an identification card carried by each of said vendees containing prerecorded vendee identification data; pluralities of vouchers carried by member vendors for recording purchase amounts; and a portable unit to be carried by each of said vendees for making purchases, said portable unit including a keyboard for manually entering transaction and identification data, terminal means accessible by only the sponsoring institution for receiving an initial funds balance corresponding to initial credit; means coupled to said terminal means for storing a funds balance; means responsive to said keyboard for storing a requested transaction amount; means for storing vendee identification data issued by said institution; means responsive to said keyboard for storing vendee entered identification data; means for comparing said stored identification data with said keyboard entered identification data and for generating a first signal in response to a positive comparison; means for comparing said stored funds balance with said requested transaction amount and for generating a second signal if said funds balance is at least as large as said requested transaction amount; an inlet for receiving singly said vouchers issued by the vendor; manually actuated printing roll means within said inlet for printing encoded identification data onto said voucher to verify the transaction; said

BUREAU OMPI WIPO INTERNATIONAL

printing roll means including means for maintaining said printing roll means normally out of contact with said voucher, means for manually moving said printing roll means into contact with said voucher, means responsive to said manual means and to said first and second signals for updating said stored funds balance by said requested transaction amount, and display means for displaying said stored funds balance and said requested transaction amount.

3. The apparatus of claim 1 or claim 2, wherein said printing roll means includes a roll containing longitudinally spaced apart bands having widths and interband spacings corresponding to said encoded identification data.

4. The apparatus of claim 1, wherein the portable unit includes a second inlet for receiving at least an edge portion of an encoded card, means within said second inlet for reading data on said card, means for comparing said card read data with prerecorded data and means responsive to said comparing means for enabling said keyboard.

5. The apparatus of claim 2, wherein said portable unit includes a second inlet for receiving at least an edge portion of said identification card, means within said second inlet for reading data on said card, means for comparing said card data with prerecorded data and means responsive to said comparing means for enabling said keyboard.

6. The invention of claim 4 or claim

BUREAU OMPI WIPO INTERNATIONAL

5, including means responsive to said card reading means for displaying data corresponding to card read data to be recorded by said vendor.

7. The invention of claim 1 or claim 2, wherein said display means includes a numerical readout for displaying stored numerical data.

8. The apparatus of claim 7, wherein said display means further includes status lamps for indicating an operating status of said microprocessor.

9. An apparatus for transferring funds data in lieu of cash, comprising a portable unit to be carried by a vendee, said portable unit including a keyboard for manually entering transaction identification data, terminal means accessible only by an authorized institution for receiving an initial funds balance, means coupled to said terminal means for storing a funds balance, means responsive to said keyboard for storing a requested transaction amount, means for storing vendee identification data issued by said institution, means responsive to said keyboard for storing vendee entered identification data, means for comparing said stored identification data with said keyboard entered identification data and for generating a first signal in response to a positive comparison, means for comparing said stored funds balance with said requested transaction amount and for generating a second signal if said funds balance is at least as large as said requested transaction amount, a first inlet for receiving at least an edge portion of an identification

BUREAU OMPI WIPO INTERNATIONAL

card, means within said first inlet for reading data prerecorded on said card, means for comparing said card read data with stored data, means responsive to said card data comparing means for enabling said keyboard, a second inlet for receiving a voucher issued by a vendor, manually actuated printing means within said second inlet for printing encoded identification data onto said voucher to verify the transaction, and means responsive to said printing means and to said first and second signals for up-dating said stored funds balance by said requested transaction amount.

10. The apparatus of claim 9, including display means for displaying said stored funds balance and said requested transaction amount.

11. The apparatus of claim 9, including means for displaying a number related to the card read data, the vendor recording said displayed number on said voucher to complete verification of said transaction.

12. A system for identifying an individual as being authorized to overcome a general restriction, comprising an identification card carried by each authorized individual containing prerecorded identification data, pluralities of vouchers located at verification stations and a portable unit to be carried by each authorized individual, each said portable unit including a keyboard for manually entering identification data, means for storing prerecorded identification data, means for storing changable data, means responsive to said keyboard and to said stored identification data for making a comparison between the keyboard

BUREAU OMPI WIPO INTERNATIONAL

entered identification data and stored identification data, a first inlet for receiving at least an edge portion of said identification card, means within said first inlet for reading encoded data on said card, means for comparing said card read data with corresponding prerecorded card data, means responsive to said card data comparing means for enabling said keyboard, a second inlet for receiving vouchers, printing means within said second inlet for printing verification data on said vouchers and means responsive to said printing means and said first comparing means for up-dating said stored changable data.

13. The invention as defined in any of claims 1, 2, 9 or 12 including a flap for enclosing said print roll inlet, said flap being biased into a position to disable said printing roll means in the absence of a voucher.

BUREAU OMPI WIPO INTERNATIONAL

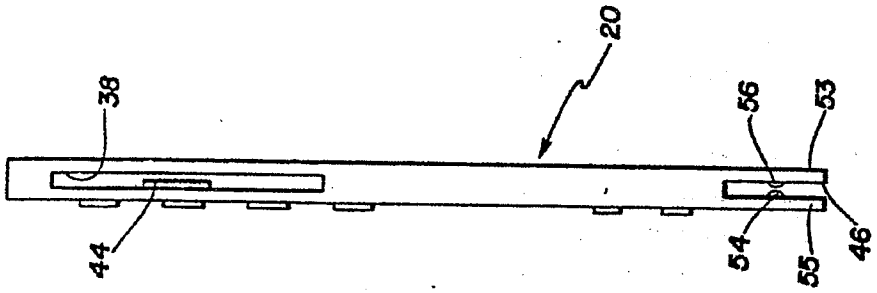


FIG.3

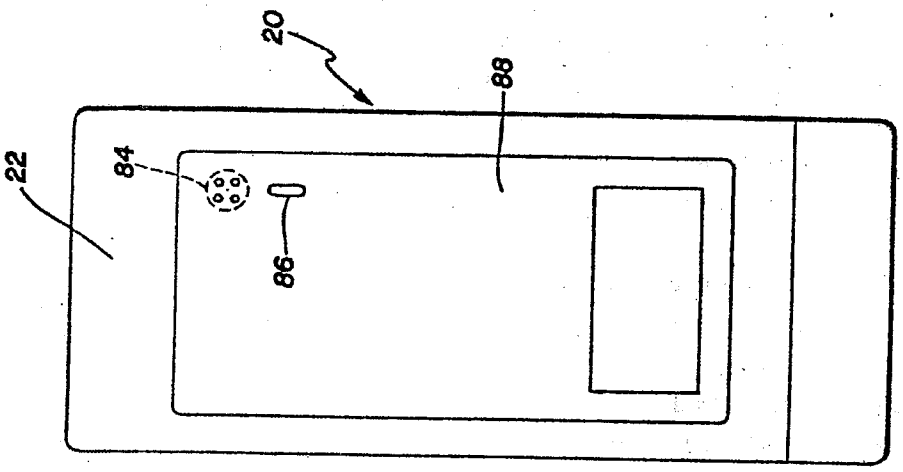


FIG.2

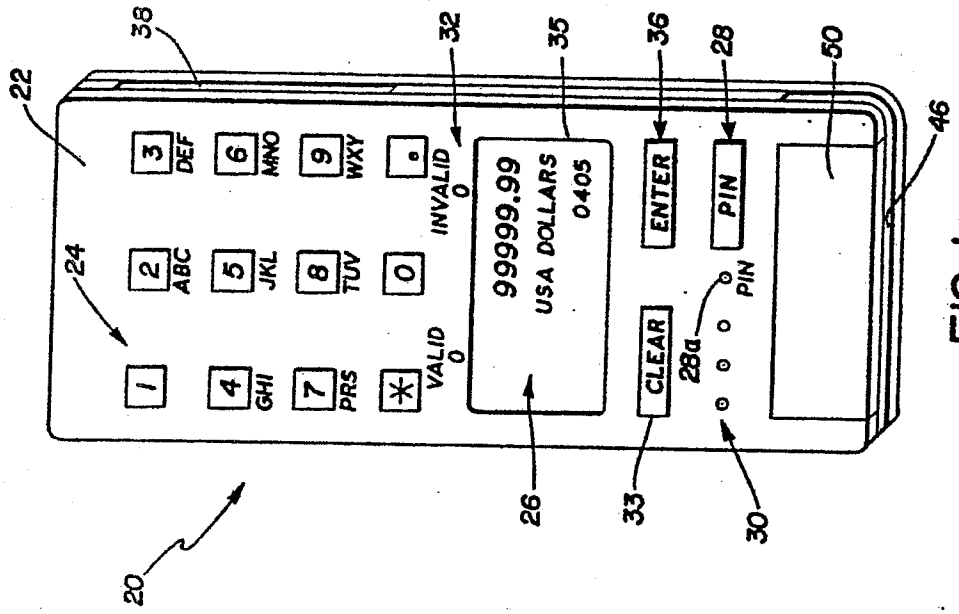


FIG. 1

BUREAU OMPI WIPO INTERNATIONAL

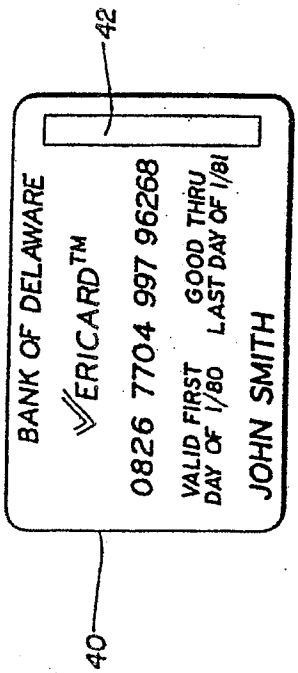


FIG. 5

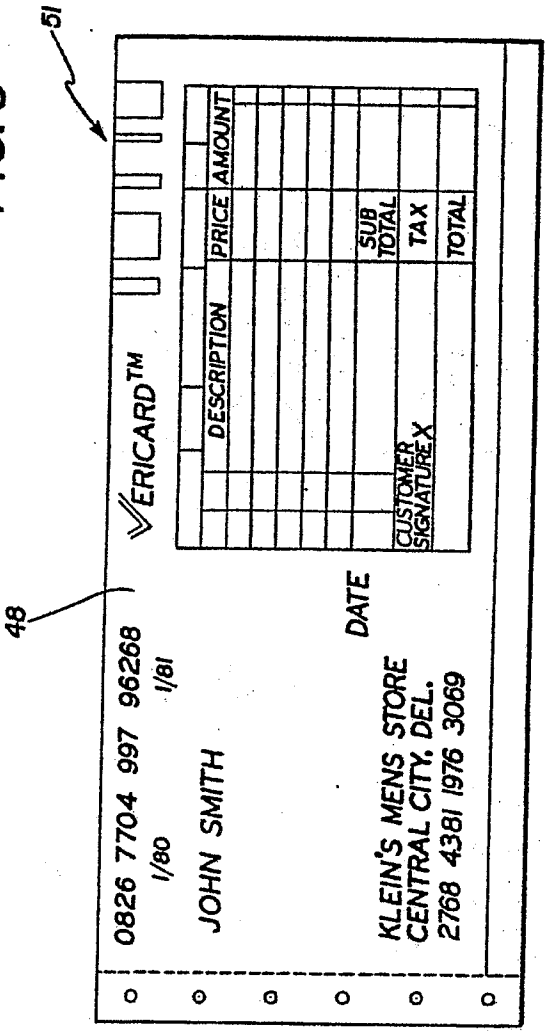


FIG.6

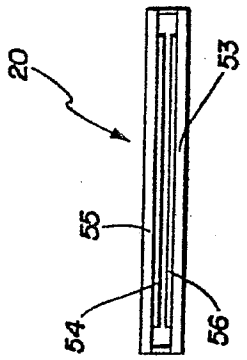


FIG. 4

BUREAU OMPI WIPO INTERNATIONAL

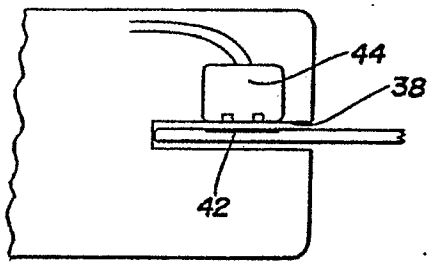


FIG. 7

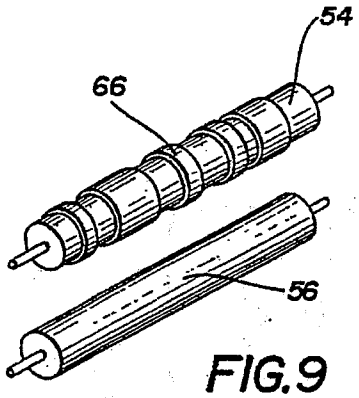


FIG. 9

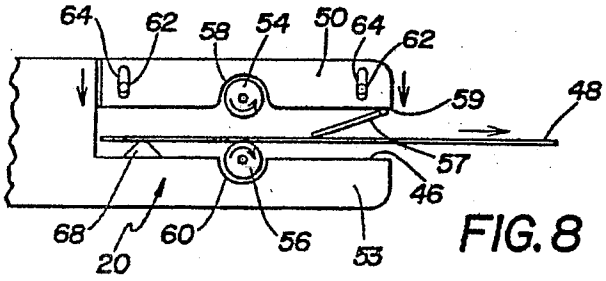


FIG. 8

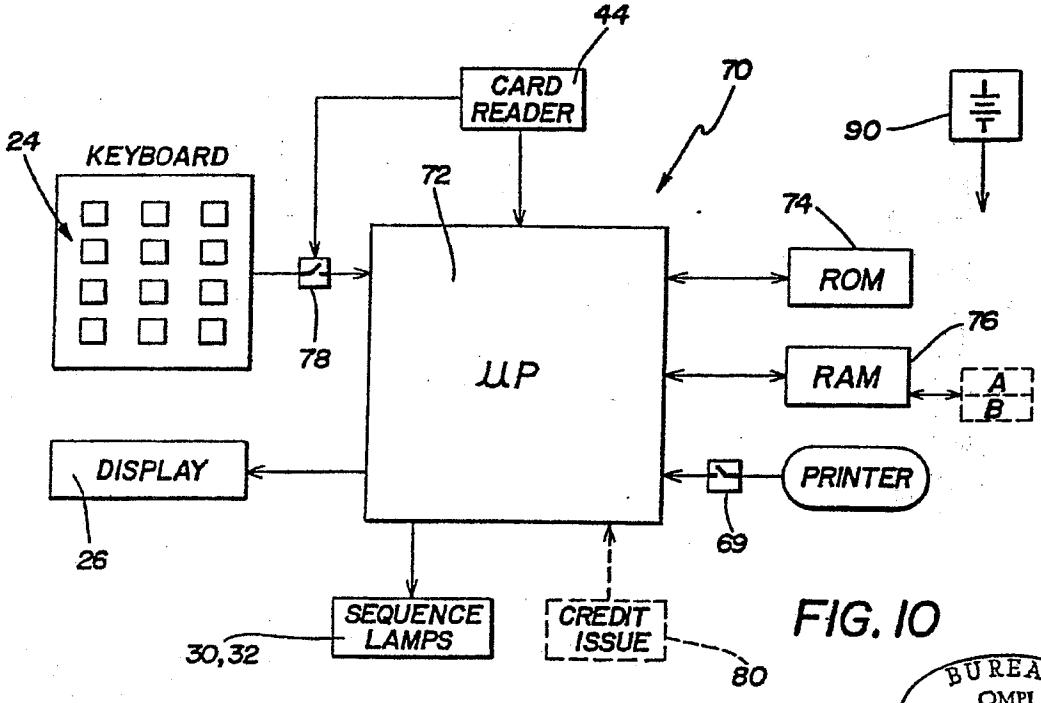


FIG. 10

BUREAU OMPI WIPO INTERNATIONAL

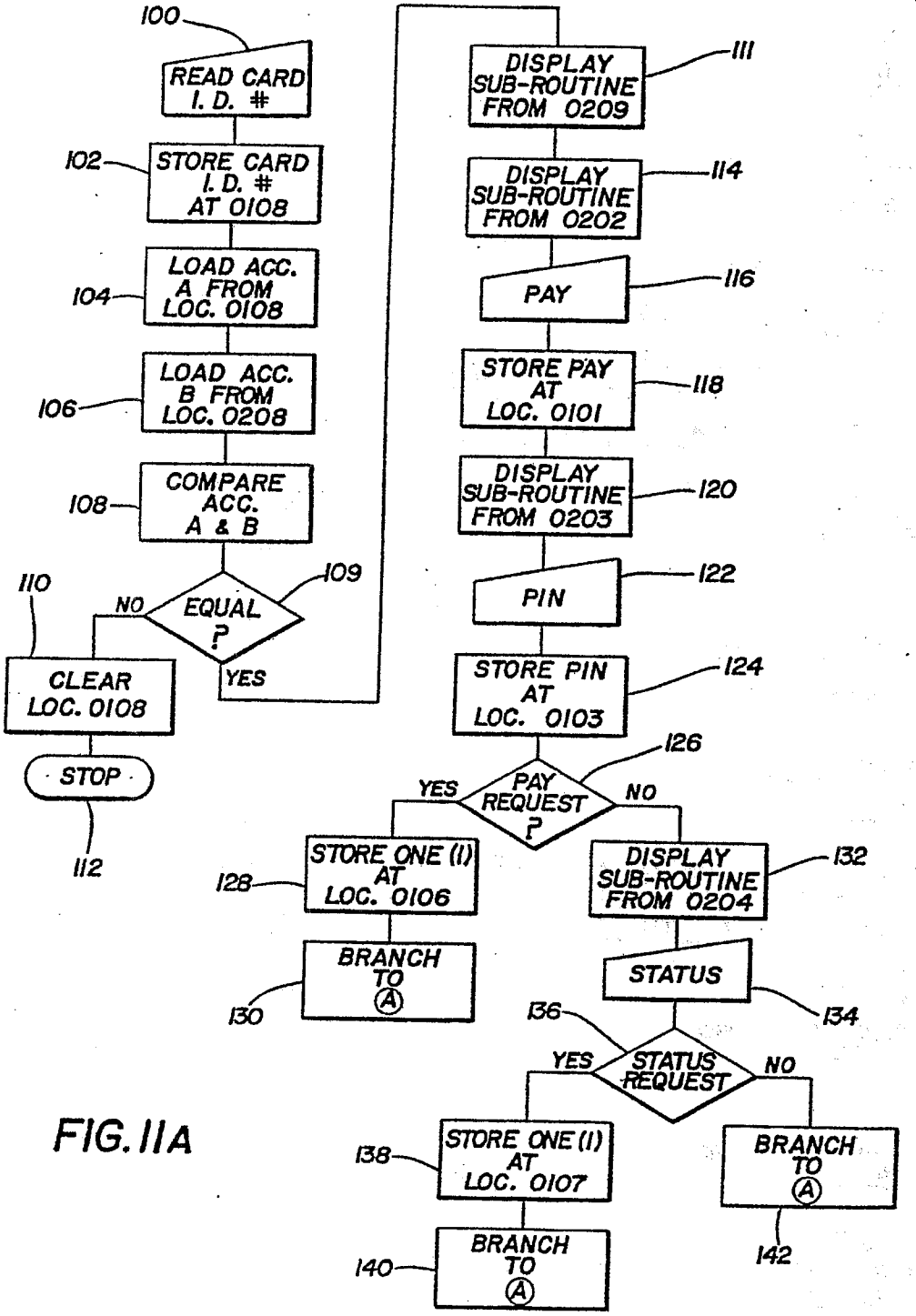


FIG. 11A

BUREAU OMPI WIPO INTERNATIONAL

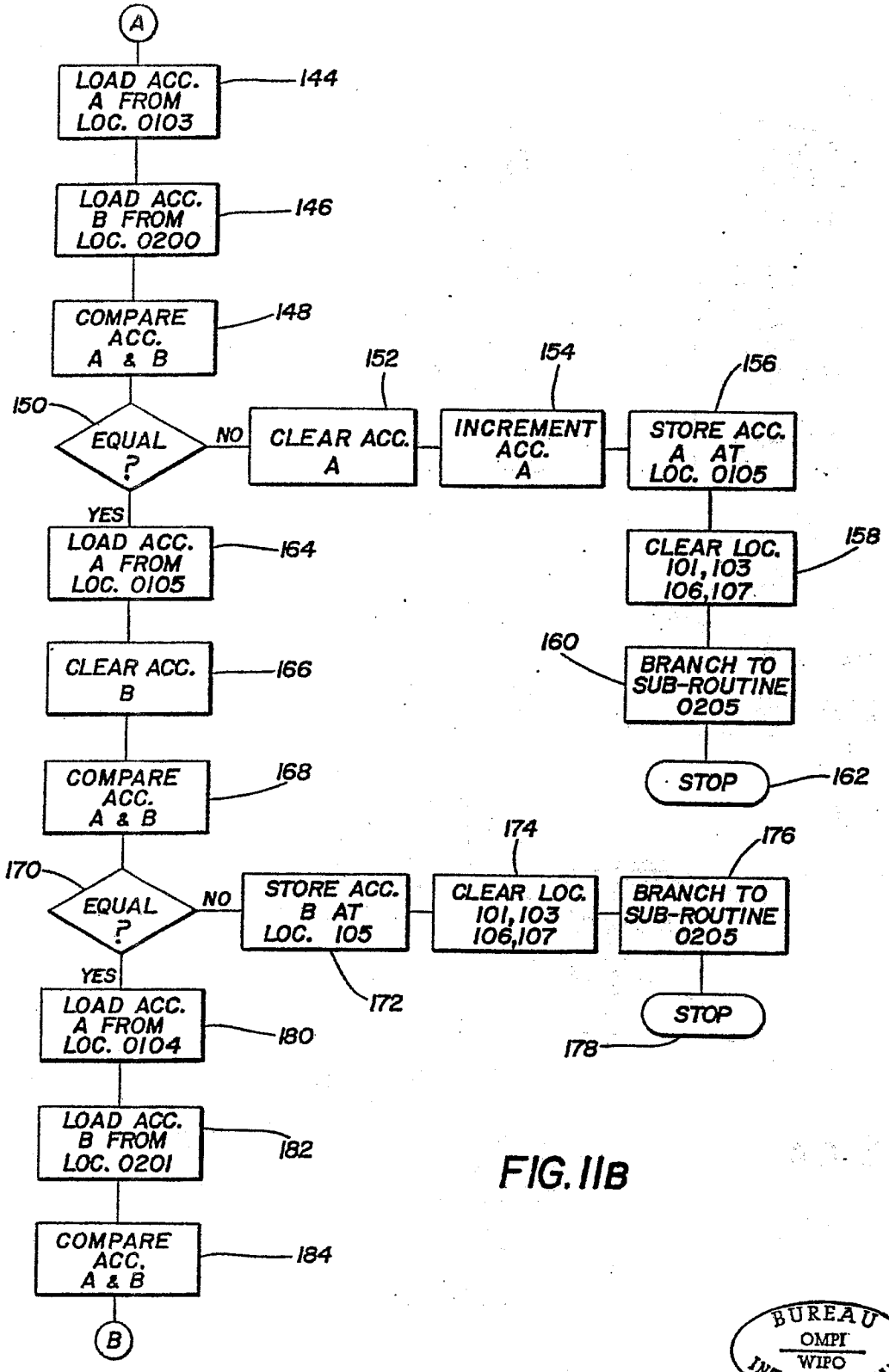


FIG. 11B

BUREAU OMPI WIPO INTERNATIONAL

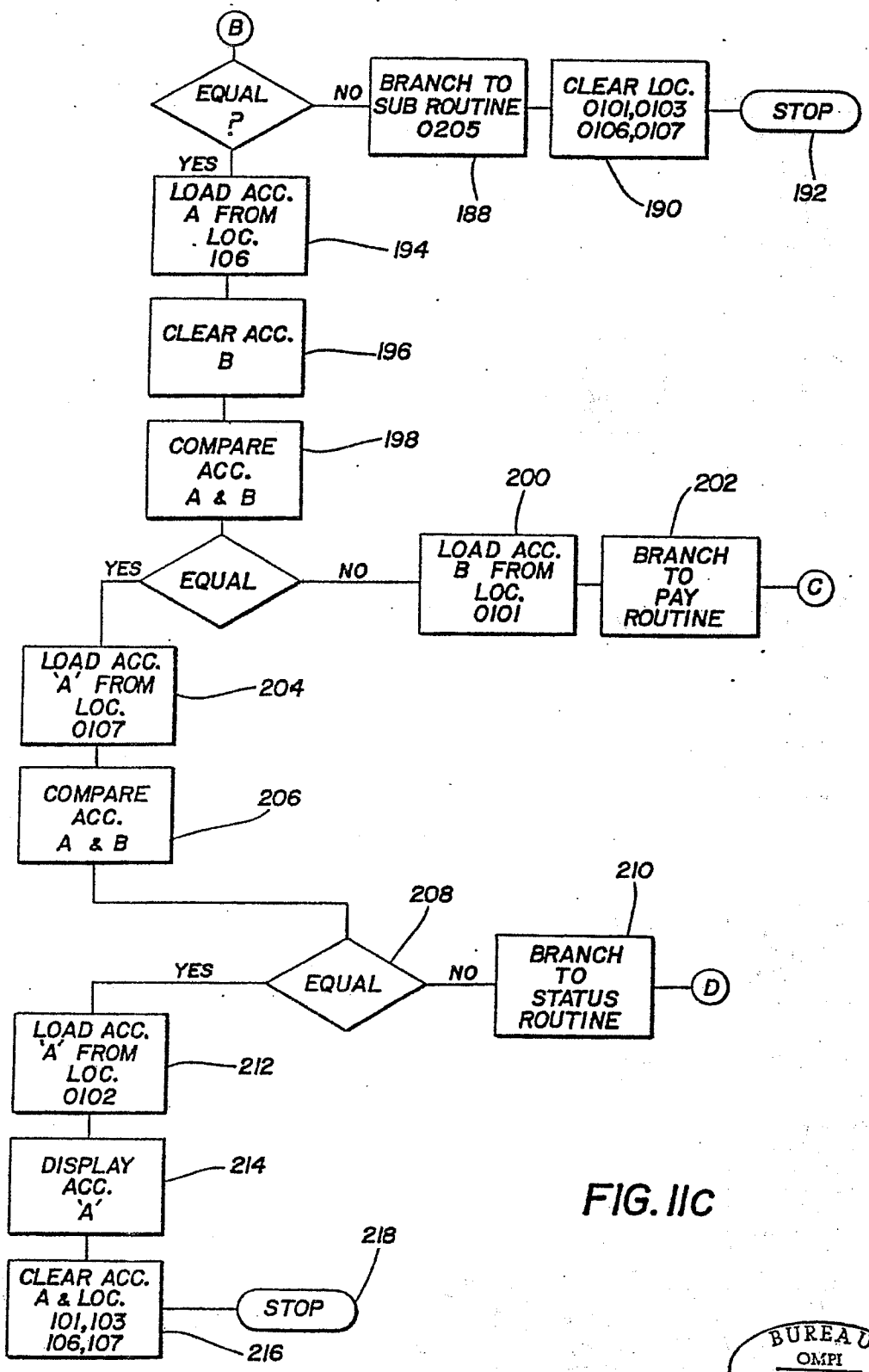


FIG. IIC

BUREAU OMPI WIPO INTERNATIONAL

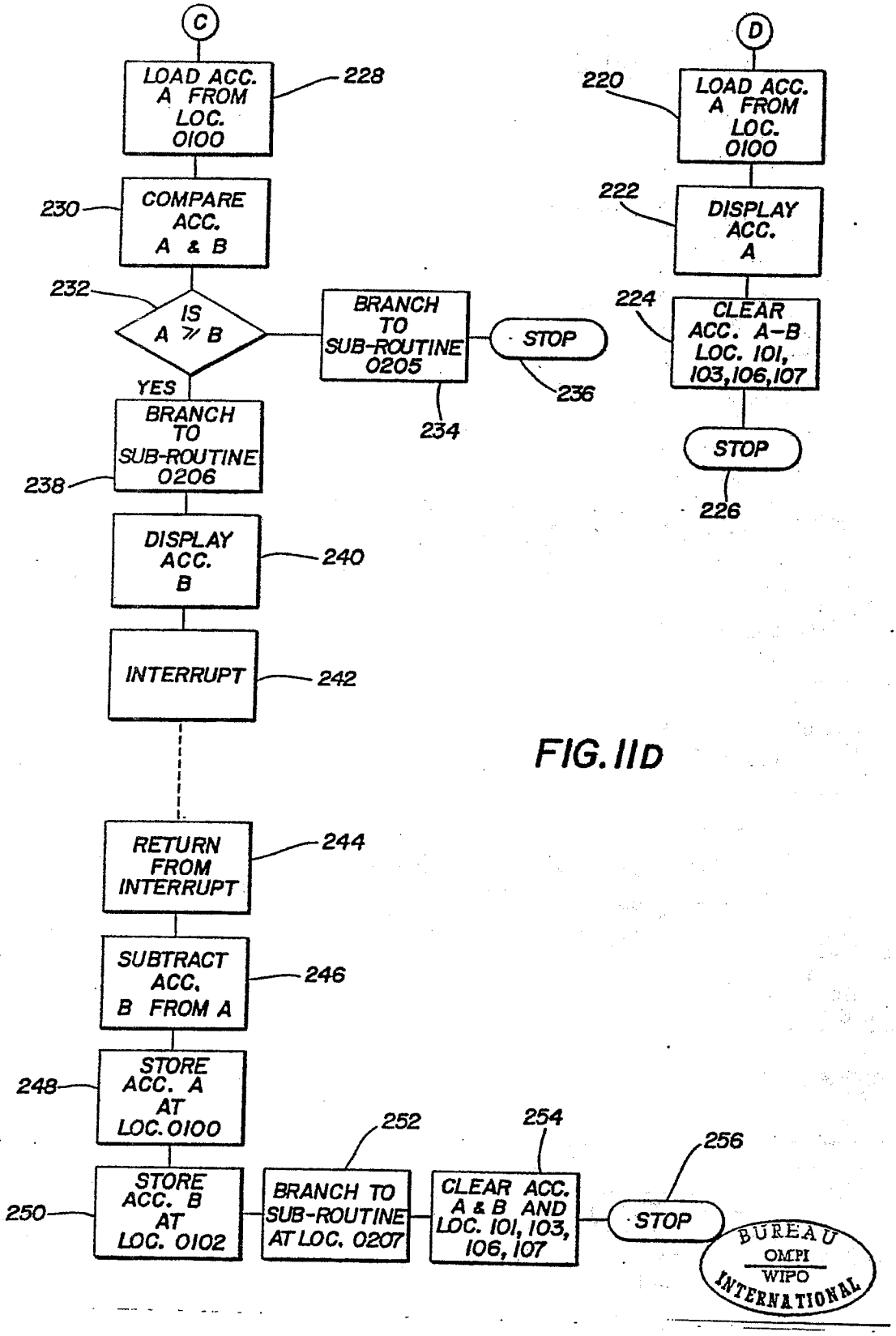


FIG. IID

BUREAU OMPI WIPO INTERNATIONAL

INTERNATIONAL SEARCH REPORT

International Application No PCT/US81/00431

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [3]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int. Cl.[3] G06 F 15/30; G06K 5/00
U.S. Cl. 235/379

II. FIELDS SEARCHED

Minimum Documentation Searched [4]

Classification System	Classification Symbols
U.S.	235/379,380,382,432; 340/149R, 149 A, 318 152;364/401,406,518,708,709,710

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [5]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [14]

Category *	Citation of Document, [16] with indication, where appropriate, of the relevant passages [17]	Relevant to Claim No. [18]
A	US, A, 3,651,310, Published 21 March 1972, Link.	
A	US, A, 3,934,122, Published 20 January 1976, Riccitelli	
A	US, A, 3,982,103, Published 21 September 1976 Goldman	
A	US, A, 4,001,550, Published 04 January 1977, Schatz	
A	US, A, 4,007,355, Published 08 February 1977, Moreno	
A	US, A, 4,032,931, Published 28 June 1977, Haker	
A	US, A, 4,053,735, Published 11 October 1977, Foudos	
A	US, A, 4,105,156, Published 08 August 1978, Dethloff	

* Special categories of cited documents: [15]

"A" document defining the general state of the art

"E" earlier document but published on or after the international filing date

"L" document cited for special reason other than those referred to in the other categories

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but on or after the priority date claimed

"T" later document published on or after the international filing date or priority date and not in conflict with the application, but cited to understand the principle or theory underlying the invention

"X" document of particular relevance

IV. CERTIFICATION

Date of the Actual Completion of the International Search [2]	Date of Mailing of this International Search Report [2]
13 July 1981	04 AUG 1981
International Searching Authority [1]	Signature of Authorized Officer [20]
ISA/US	Thomas A. Robinson

Form PCT/ISA/210 (second sheet) (October 1977)

FURTHER INFORMATION CONTINUED FROM THE SECOND SHEET

A	US, A, 4,115,870, Published 19 September 1978, Lowell
A	US, A, 4,172,552, Published 30 October 1979, Case et al
A	US, A, 4,197,986, Published 15 April 1980, Nagata

V. ☐ OBSERVATIONS WHERE CERTAIN CLAIMS WERE FOUND UNSEARCHABLE [10]

This international search report has not been established in respect of certain claims under Article 17(2) (a) for the following reasons:

1. ☐ Claim numbers _____, because they relate to subject matter [12] not required to be searched by this Authority, namely:

2. ☐ Claim numbers _____, because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out [13], specifically:

VI. ☐ OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING [11]

This International Searching Authority found multiple inventions in this international application as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims of the international application.

2. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims of the international application for which fees were paid, specifically claims:

3. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim numbers:

Remark on Protest

☐ The additional search fees were accompanied by applicant's protest.

☐ No protest accompanied the payment of additional search fees.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :
G07B 1/02, G07F 17/42
G06F 15/24

A1

(11) International Publication Number: **WO 92/15968**

(43) International Publication Date: 17 September 1992 (17.09.92)

(21) International Application Number: PCT/US92/01187

(22) International Filing Date: 12 February 1992 (12.02.92)

(30) Priority data:

664,930	5 March 1991 (05.03.91)	US
760,875	16 September 1991 (16.09.91)	US

(71) Applicant: THE GIFT CERTIFICATE CENTER, INC. [US/US]; 3800 West 80th Street, Minneapolis, MN 55431 (US).

(72) Inventors: VEENEMAN, William, J. ; 4600 DuPont Avenue South, Minneapolis, MN 55409 (US). ALEXANDER, Karla, J. ; 4109 Williston Road, Minnetonka, MN 55345 (US). DOYLE, Thomas, J. ; 5317 James Avenue South, Minneapolis, MN 55419 (US). BROOKS, Phillip, R. ; 4046 Deerwood Trail, Eagan, MN 55122 (US). HAMILTON, Robert, H. ; 5010 Arden Avenue, Edina, MN 55424 (US).

(74) Agent: HAMRE, Curtis, B.; Merchant, Gould, Smith, Edell, Welter & Schmidt, 3100 Norwest Center, 90 South Seventh Street, Minneapolis, MN 55402 (US).

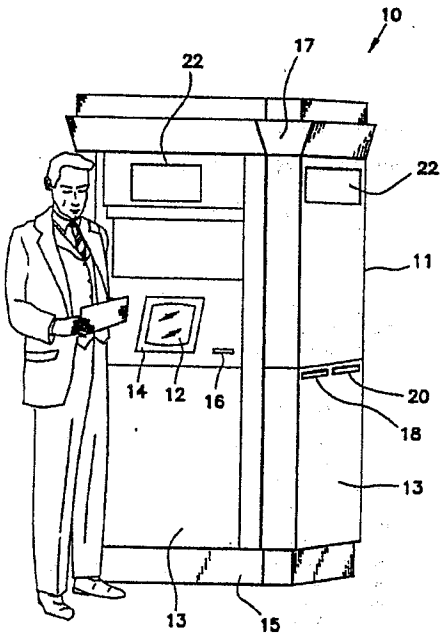
(81) Designated States: AT (European patent), AU, BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, KR, LU (European patent), MC (European patent), NL (European patent), SE (European patent).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR GENERATING GIFT CERTIFICATES

(57) Abstract

An electronic gift certificate dispenser device (10) for printing and dispensing a gift certificate purchased by a credit card. A consumer approaches the device (10) and inserts a credit card into a magnetic card reader (16). The consumer chooses a retailer from a menu of participating retailers and enters the gift certificate value. The machine automatically verifies the credit card, causes the account to be debited and prints the gift certificate (200). A plurality of gift certificate dispensing devices (10.1....10.N) can be connected in a network under the control of a central processing unit (10). Information regarding gift certificate pruchases is transferred from the devices (10.1...10.N) to the central processing unit (60) to be collated and billed to credit card accounts. The central processing unit (60) also informs merchants of the purchase of gift certificates that will be redeemed at their stores.



JUMBO PATENT
DUE TO ITS EXCESSIVE LENGTH,
COMPLETE PATENT FURNISHED
UPON SPECIAL REQUEST ONLY.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FI	Finland	ML	Mali
AU	Australia	FR	France	MN	Mongolia
BB	Barbados	GA	Gabon	MR	Mauritania
BE	Belgium	GB	United Kingdom	MW	Malawi
BF	Burkina Faso	GN	Guinea	NL	Netherlands
BG	Bulgaria	GR	Greece	NO	Norway
BJ	Benin	HU	Hungary	PL	Poland
BR	Brazil	IE	Ireland	RO	Romania
CA	Canada	IT	Italy	RU	Russian Federation
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland			SN	Senegal
CI	Côte d'Ivoire	KR	Republic of Korea	SU	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
CS	Czechoslovakia	LK	Sri Lanka	TG	Togo
DE	Germany	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		
ES	Spain	MG	Madagascar		

METHOD AND APPARATUS FOR GENERATING GIFT CERTIFICATES

Background of the Invention

Field of the Invention

The present invention relates to an apparatus and method for dispensing gift certificates, and more particularly to an apparatus and method for vending such certificates from terminals in communication with a central processing mechanism.

Background of the Invention

Due to increasing time constraints in the lives of busy people, gift certificates have emerged as a viable alternative to the purchase of the gift itself. Gift certificates offer many advantages over the purchase of a gift. If the gift giver is unsure of the needs of the recipient, a gift certificate offers a wide range of goods or services from which the recipient can choose. Gift certificates also remove the hassle of exchanging a gift without a receipt.

Currently gift certificates can be purchased only at retail locations or through catalog houses. This makes the purchase of a certificate less convenient and, therefore, reduces its value to the consumer.

A similar convenience problem was recognized and addressed in the banking industry. One of the solutions was the development of Automatic Teller Machine (ATM) devices. ATMs have become popular for handling simple repetitive transactions such as the dispensing of currency. The widespread acceptance of ATMs has created an educated consumer willing to conduct transactions through a vending device accessed by a credit card.

A similar type of device has been applied to the airline ticketing industry. U.S. Patent No. 4,818,854, issued to Davies et al. discloses an

automatic ticket handling machine used for vending airline tickets. The consumer approaches the machine, inserts a credit card into the card reader, enters a ticketing request through a touch screen and receives a printed ticket. The machine automatically verifies the credit card and debits the account.

The gift certificate industry has special requirements that make development of an automatic transaction machine difficult. Gift certificates are similar to currency in their ease of use and anonymity. Steps must be taken to prevent the use of stolen credit cards in the procurement of certificates and to secure paper stock to make forging of certificates difficult.

It is apparent that there is a need for a device that can dispense gift certificates while maintaining a high level of security.

Summary of the Invention

The present invention provides a device incorporating a magnetic card reader, a control mechanism and a printer for the printing and dispensing of gift certificates. The consumer approaches the device and chooses a retailer from a menu of participating retailers and enters the gift certificate value. The device automatically verifies a credit card inserted into a card reader, and, on receiving a final validation from the consumer, causes the credit card account to be debited and prints the gift certificate.

According to another embodiment of the present invention, a plurality of devices for printing and dispensing gift certificates are connected to a central processing unit. Each device must establish communication with the central processing unit before it can become operative. At any time after a device becomes operative, it can be rendered inoperative by command from the central processing unit.

According to yet another embodiment of the present invention, a device is disclosed for dispensing gift certificates. Users of the device enter instructions at a first wall of the device. Finished gift certificates and envelopes are delivered at slots in a second wall.

According to yet another embodiment of the present invention, a device is disclosed for dispensing gift certificates comprising a redeemable section and a receipt. The redeemable section includes a holographic foil to make counterfeiting difficult.

According to yet another embodiment of the present invention, a method is disclosed for controlling the selection and printing of gift certificates from a network of gift certificate dispensing terminals connected to a central processing unit.

According to yet another embodiment of the present invention, a method is disclosed for controlling access to the electronics of a device used for printing and dispensing a gift certificate.

According to another aspect of the present invention, to discourage credit card fraud each device monitors credit cards used within a predetermined period and limits the total value that can be charged to a credit card within that period to a predetermined maximum value within that period.

Brief Description of the Drawings

FIG. 1 is a perspective view of a gift certificate dispensing device in accord with the present invention.

FIG. 2 is an electrical block diagram representation of the gift certificate dispensing device according to the present invention.

FIG. 3 is an alternative electrical block diagram representation of the gift certificate dispensing device according to the present invention.

FIG. 4 is a block diagram representative of a network of gift certificate dispensing devices coordinated by a main computer and one or more credit card authorization computers according to the present invention.

FIGS. 5a and 5b are flow chart representations of the steps taken in initializing the gift certificate dispensing device computer upon power up.

FIG. 6 is a flow chart representation of the steps taken in shutting down the system after a hard failure.

FIG. 7 is a flow chart representation of the steps taken in initiating a call to an external computer system.

FIG. 8 is a flow chart representation of the steps taken in validating a credit card with a credit authorization computer.

FIG. 9 illustrates a series of representations of the screen images that are displayed according to the present invention to attract consumer attention and to explain the operation of the gift certificate dispensing device.

FIG. 10a is a flow chart representation of the screens that are displayed as a consumer selects a retailer according to the present invention.

FIGS. 10b and 10c are flow chart representations of the screens that are displayed as a consumer selects a gift certificate for a previously selected store according to the present invention.

FIG. 11 is a flow chart representation of the screens that are displayed as a response to a customer selecting the BROWSE option during the "Select a Store" phase according to the present invention.

FIG. 12 is a representation of a gift certificate in accord with the present invention.

FIG. 13 is a front view of an alternate embodiment of a housing for a gift certificate dispensing device in accord with the present invention.

FIG. 14 is a side view of the device in FIG. 13.

FIGS. 15a and 15b are flow chart representations of the steps taken in capturing a signature.

Detailed Description of the Preferred Embodiments

In the following Detailed Description of the Preferred Embodiments, reference is made to the accompanying Drawings which form a part hereof, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. Like numerals throughout the several views identify like features, the like numerals being primed in alternate embodiments. It is to be understood that other embodiments may also be possible and may be utilized and structural changes may be made without departing from the scope of the present invention.

An electronic gift certificate dispensing device 10 is shown in FIG. 1. Gift certificate dispensing device 10 is a stand-alone housing 11 having a rectangular shape with panel-like walls 13, a base 15 and a top 17. Dispensing device 10 houses a monitor 12 with touch screen 14, a magnetic card reader 16, a certificate dispenser slot 18, an envelope dispenser slot 20 and identifying plaques 22 on one or more sides of the device. In the preferred embodiment plaque 22 is made of a backlit translucent material with indicia thereon. Ventilation for the interior of the housing is provided by means of a fan or air conditioner (not shown).

Monitor 12 is used to display choices given to the customer in the purchase of a gift certificate. Choices are made by the customer and entered by touching predetermined areas of touch screen 14. Card reader 16 is used to swipe a credit card in order to debit a credit card account for payment for gift certificates dispensed. It should be noted that although the preferred embodiment is geared toward the use of a credit card it should be obvious that the teaching of the present invention could easily be applied to a debit card system or to a system which accepts cash.

In one embodiment, and as shown in FIG. 1, monitor 12, touch screen 14 and card reader 16 are mounted in a first wall of the housing 11 of device 10. Certificate dispenser slot 18 and envelope dispenser slot 20 are mounted in a second wall of device 10. A customer will approach touch screen 14 in the first wall, enter gift certificate choices, swipe a credit card through card reader 16 and then step to the second wall to await printing and dispensing of the certificate and envelope. This allows a second customer to approach device 10 while the first customer is waiting for his transaction to finish.

In a second embodiment, the plaque 22 positioned over certificate dispenser slot 18 and envelope dispenser slot 20 is replaced by a monitor (not shown) used for displaying messages such as instructions or advertising to a person waiting for a certificate to issue.

In a third embodiment, dispensing device 10 is built into a wall or like structure and covered by one or more panel-like wall portions 13 housing a card reader 16, a certificate dispenser slot 18, an envelope dispenser slot 20 and a monitor 12 with touch screen 14 mounted thereon.

In a fourth embodiment, as shown in FIGS. 13 and 14, housing 11' of a device 10' includes a user access subhousing 600 and an electronics mounting subhousing 602. User access subhousing 600 includes a front panel-like wall portion 604 which is separated into a plurality of sections for ease of use by the user, even a user in a wheelchair. Panel-like wall portion 604 includes an upper section 606 having a lighted display 608 therein. An inclined section 608 extends forwardly from section 606 such that the front screen of monitor 12' is mounted in it with touch screen 14' appropriately installed thereto. In an inset portion having a vertical wall 610 with a horizontal surface therebelow, the card reader 16' is mounted with an appropriate receiving slot in vertical wall 610. A section 612 then extends inwardly from the front edge of section 608 to one or more additional sections leading to the bottom of subhousing 600.

The front panel-like wall portion 614, which may also be the electronics access door, of subhousing 602 is essentially vertical. Certificate dispenser slot 18' and envelope dispenser slot 20' are located in panel-like wall portion 614.

Section 606 of wall portion 604 is considerably offset rearwardly from panel-like wall portion 614.

There is then a connecting wall 616 appropriate for mounting a speaker 618.

In this way, a user approaches panel-like wall portion 604 and can readily read lighted display 608, operate touch screen 14', activate device 10' with an appropriate card at card reader 16', and be in a good position to listen to any instructions projecting from speaker 618. The sections of wall portion 604 beneath section 612 are sufficiently inset so that a person in a wheelchair can position relative to wall portion 604 adequately so that if the person is otherwise capable, should be able to interact with device 10' as indicated. After an appropriate order has been placed, the person can then move aside from panel-like wall portion 604 to wait for the ordered gift certificate and envelope to be dispensed from gift certificate dispenser slot 18' and envelope dispenser slot 20' in adjacent panel-like wall portion 614.

The various electronics which provide the advantageous features of gift certificate dispensing device are secured in the housing of the dispensing device. FIG. 2 shows an electrical block diagram of electronic gift certificate dispensing device in accordance with the present invention. Computer 24 is connected to monitor 12, touch screen 14, keyboard 19, nonvolatile memory device 28, expander device 30, security interface 33, modem 42 and voice playback 48. Expander device 30 is connected to envelope dispenser 32, laser printer 26 and card reader 16. Security interface 33 is connected to temperature sensor 36 and various security items (not shown). Expander device 30 and security interface 33 are interface circuits with registers that receive commands from computer 24 and transmit status back to computer 24. Voice playback 48 is connected through amplifier 50 to speaker 23. Voice playback 48 synthesizes voice messages in response to commands received from computer 24. Modem 42 is

connected through internal telephone jack 44 to public telecommunications channel 46.

In the preferred embodiment, computer 24 is an IBM PC or compatible computer with at least 2 MBytes of dynamic memory. Monitor 12 is a standard super VGA monitor capable of displaying 640 X 480 pixels at 256 colors per pixel. Touch screen 14 is an Elographics Intellitouch Model 4001 surface acoustic wave touch screen with touch screen controller. Card reader 16 is a MAGTEX 21055002 slotted magnetic card reader connected to computer 24 through an RS232 line. Laser printer 26 is a Canon LBP4 laser printer. Nonvolatile memory device 28 is a 40 MByte fixed disk drive. Modem 42 is a 2400 Baud MNP Level 5 error correcting modem. Voice playback 48 is manufactured by COVOX. In an alternate embodiment voice playback 48 is replaced by an audio synthesizer capable of creating voice and music from data stored in computer 24. Telephone jack 44 is a standard jack compatible with a standard domestic telephone cable. All these items are commercially available as is known to those skilled in the art.

Card reader 16 is a typical magnetic card reader used to read coded data stored in a magnetic strip on a credit or debit card. Credit cards and debit cards typically have information such as the account name, the account number and the expiration date of the card encoded and deposited on their magnetic strip. Card readers such as card reader 16 contain circuitry which reads the encoded data and sends that data to computer 24 for use in validating the card.

An alternate embodiment of the electronics of a gift certificate dispensing device 10 is shown in FIG. 3. In FIG. 3 a card reader 50 with integral modem is used to automatically dial a credit card service for verification of a credit card passed therethrough. A telephone switch 52 under control of peripheral control device 30 connects the modem in card reader 50 to public

telecommunications channel 46. This embodiment offloads some of the processing required by computer 24 at the cost of a more expensive card reader and some commercially available switching logic. The embodiment shown in FIG. 3 does not have the voice synthesizing circuitry shown in FIG. 2. Although tests have shown a synthesizer effect between the screen displays on monitor 12 and the voice messages generated by playback 48, a design decision may be made to remove the synthesizer circuitry to reduce system cost. All other electronics are the same as in FIG. 2.

In yet another alternate embodiment (not shown), a second monitor, a second touch screen and a second card reader are mounted on the wall 13 opposite monitor 12. The second monitor, the second touch screen and the second card reader are connected to computer 24 such that a second terminal is provided for selecting and printing gift certificates. Computer 24 controls the operation of both sets of monitors, touch screens and card readers as two separate tasks. Access to common resources such as laser printer 26 and modem 42 is arbitrated by computer 24. Envelopes and printed gift certificates are still dispensed through slots 20 and 18, respectively.

In the preferred embodiment access to the electronics of dispensing device 10 is limited. Only touch screen 14 and card reader 16 are readily accessible to the user. The remainder of the electronics are secured behind the access door.

Also, in the preferred embodiment, temperature sensor 36 mounted inside gift certificate dispensing device 10 measures the ambient temperature within dispensing device 10 and reports that temperature to computer 24. If the measured ambient temperature rises above 85 degrees Fahrenheit computer 24 automatically shuts down the electronics of device 10 to avoid damage to electronic components.

Gift certificate dispensing device 10 can operate independently or within a network. Networked operation of the dispensing devices is preferred since it eases the requirement for local security. In the preferred embodiment a number of gift certificate dispensing devices 10 are connected by telephone to a main computer. The main computer can poll dispensing devices to determine if a dispensing device has been disconnected or has lost power, can execute diagnostic tests remotely to expedite detection of hardware failure and can monitor devices for unauthorized access or vandalism.

FIG. 4 is a block diagram representative of a network of gift certificate dispensing devices 10 coordinated by a main computer. In FIG. 4, gift certificate dispensing devices 10.1 through 10.N are connected through public telecommunications channel 46 to main computer 60. Transactions entered at one of the devices 10 are transmitted to computer 60 over channel 46. Computer 60 in turn accesses one or more credit card authorization computers 62.1 through 62.M through channel 46 to receive credit card authorization. Authorization is then granted by computer 60 to the appropriate dispensing device 10.

Computer 60 is connected to a printer 64 for printing transactions either as they occur or as a batch at predetermined time intervals. In the preferred embodiment computer 60 is a PC compatible computer. Purchases made through gift certificate dispensing devices 10. 1 through 10.N are accumulated in computer 60. Requests for payment (debits to credit card accounts) for those purchases are either submitted electronically through public telecommunications channel 46 to computer 62 or submitted as a bill printed from printer 64. In a like manner, merchants are notified of purchases of gift certificates issued in their name and of the code numbers of the certificates issued either

through channel 46 or through a report printed by printer 64.

Steps have been taken to ensure secure operation of gift certificate dispensing devices 10. In the preferred embodiment, device 10 powers up inoperative. In order to become operative, it must establish communication with computer 60, download a unique security code and appropriately verify that code.

Computer 60 can at any time render any device 10 in the network inoperative by sending it a shut down command. Reception of the shut down command causes a device 10 to destroy sensitive program code and data and enter a special system shut down routine that disables the user interface. A representative system shut down routine is shown in FIG. 6 and described later. This is a useful security feature that can be used to disable a device 10 when computer 60 detects a failure or impending failure.

Gift certificates are printed with an intricate multicolored design on faded parchment paper and embossed with holographic foil. The type of paper, the ink and the amount of detail are chosen to make copying difficult. Embossing the certificate with holographic foil makes counterfeiting more difficult. In the preferred embodiment, the holographic foil may be obtained from and applied by Larkin Industries, St. Paul, Minnesota.

A representative gift certificate is shown in FIG. 12. Gift certificate 200 is a standard size sheet of faded parchment paper divided into three sections 202, 204 and 206 with perforations 208 for easy separation of the sections. Section 202 is used to print a receipt for the transaction. The name and account number on the credit card is printed along with name of the recipient, the date, the charges for the purchase and the dispensing device 10 from which the certificate was purchased. In the preferred embodiment,

a service charge per certificate is included in the total charges. Section 204 is used to display the name of the intended recipient, a message such as "Happy Birthday" or "Thank You" and the name of the purchaser. Section 206 is the section of the gift certificate that is redeemed to purchase merchandise from the intended retailer.

In the preferred embodiment, during production each section 206 is imprinted with a unique control code (not shown) and silver embossed with a hologram 210. The code imprinted is matched to the name of the intended recipient during the sale of the certificate and the code and the name of the recipient are then communicated to the intended retailer. When the certificate is redeemed the code can be compared against a list of expected codes and verified for authenticity. In an alternate embodiment, the control code could be implemented as a bar code that can be scanned with a bar code reader.

A logo representative of the company operating the particular gift certificate dispensing device 10 is printed at 212 and 214. A bit-mapped graphic or logo representative of the intended retailer and, if requested, a retailer control code are retrieved from nonvolatile memory device 28 and printed to location 216 of certificate 200 during certificate printing. Retailer logos are obtained by scanning a design provided by the retailer and storing the resulting image to nonvolatile memory device 28.

Purchasers receive certificate 200, remove section 202 for their records and send sections 204 and 206 to the intended recipient. The recipient receives sections 204 and 206, detaches 204 from 206 and redeems section 206 at the designated store.

Gift certificates are stored in a bonded printer. Only bonded authorized service personnel can obtain paper and install it in the printer. Supplies of

paper in each device 10 are checked randomly for integrity.

The value of a certificate 200 cannot exceed a predetermined amount. In addition, each device 10 monitors use of each credit card and prevents charging more than a predetermined limit in a designated time period. In networked systems this protection against credit card abuse can be extended to all gift certificate dispensing devices 10 in the network.

Each certificate is printed with an expiration date to encourage timely redemption. To further enhance security, participating stores are requested to redeem certificates for merchandise only and to request identification while redeeming a certificate.

In use, on receiving power, computer 24 executes a power-on self test. In a PC compatible computer this test is a resident program that is typically executed out of ROM (read only memory). The power-on self test checks system dynamic memory, the system board, nonvolatile memory device 28 and monitor 12. Upon successful completion, computer 24 reads up a portion of its programming from nonvolatile memory device 30 and begins executing a system initialization program. If computer 24 is unable to successfully complete the power-up self test, a message to that effect is displayed on monitor 12 and gift certificate dispensing device 10 is disabled.

A control flow program representative of a system initialization for the present invention is illustrated in FIGS. 5a and 5b. The routine shown is written for a networked environment. It should be obvious to one skilled in the art that this routine is readily adaptable to independent operation of a gift certificate dispensing device.

The routine is entered at 70 after successful execution of the power-on self test. First, communication is established with main computer 60. At

70 an attempt is made to initialize modem 42. At 72 a check is made to see if the modem is ready. If not, at 74 a message is displayed on monitor 12 detailing the error and requesting service.

If at 72 the modem is found to be ready, at 76 a telephone call is made to main computer 60 and a security code downloaded from computer 60 to computer 24. At 78, the downloaded security code is compared against a code stored on nonvolatile memory device 28. If the two codes match, node security has been verified. Retry count is set to zero and control moves to 82 to initialize laser printer 26. If the two codes do not match, a system shutdown routine is called at 80 to secure the gift certificate dispensing device.

After link security has been verified at 78, at 82 an attempt is made to initialize printer 26. A check is made at 84 to see if printer 26 is ready. If not, at 86 computer 24 executes a one minute wait, at 88 the retry count is incremented and at 90 a check is made to see if the number of initialization attempts equals three. If so, at 92 a telephone call is placed through modem 42 to main computer 60 and the error is logged.

If at 84 printer 26 is determined to be ready, a check is made at 94 to see if printer 26 has blank certificates. If not, control moves to 92, a telephone call is placed through modem 42 to main computer 60 and the error is logged.

If at 94 printer 26 is determined to have a supply of blank certificates, control moves to 96 where touch screen 14 is initialized. At 98 a check is made to see if touch screen 14 is ready. If not, control moves to 92 to log the error. If touch screen 14 is ready, at 100 card reader 16 is initialized and at 102 a check made to see if card reader 16 is ready. If not, control moves to 92 to log the error. If card reader 16 is ready, at 104 the main program is initiated.

On successful completion of the initialization program of FIGS. 5a and 5b, computer 24 enters the main program. The main program will now be described from the standpoint of the user interface.

The following discussion is a description of one embodiment of the screen displays and user interface for a gift certificate dispensing device. It should be understood that logical flows other than that described could be implemented without departing from the spirit and scope of the present invention. In one embodiment, the main program starts with the Attractor module shown in FIG. 9. The Attractor module is an endless loop during which a sequence of display screens is shown on monitor 12. The sequence of display screens is intended to familiarize the consumer with the gift certificate product itself and with the method used to purchase a gift certificate. The loop is terminated by the detection of a touch on touch screen 14. FIG. 9 shows a representative sequence of display screens used while waiting for the touch on touch screen 14. At 300 a welcome screen is displayed. At 302, a list of participating retailers is displayed. At 304, some examples of completed gift certificates are shown. At 306, a list of the types of credit cards that can be used is displayed. At 308, instructions on use of magnetic card reader 16 are displayed. At 310, transaction charges are explained. At 312, a graphic demonstrating design of a custom gift certificate is displayed. At 314, a graphic illustrating the printing and dispensing of a gift certificate is displayed. And at 316, a graphic describing the company that owns the particular gift certificate dispensing device is displayed (in this case the company is THE GIFT CERTIFICATE CENTER, INC. or GCC). The routine continues scrolling through screens 300 through 316 until a touch is detected on touch screen 14.

In the preferred embodiment, a combination of voice and screen messages is used to guide the customer in a purchase. Once a touch is detected, control moves to the routine shown in FIG. 10a. FIG. 10a illustrates the sequence of screen displays shown while choosing the retailer to be shown on the purchased gift certificate. The routine is entered at 320 where a screen is displayed with clearly marked areas labeled "How to use the GCC", "Browse" and "Start Shopping". At the same time a welcoming message is broadcasted over speaker 23. Computer 24 then waits for a selection made by touching within the marked areas on touch screen 14. At 320, as in the remaining screens of FIGS. 10a through 10c, if no touch is detected within a first predetermined period a prompt such as "Please touch the screen to continue" is displayed on monitor 12. A second predetermined period is allowed to pass. If no touch is detected yet, a prompt such as "Please make your selection now" is displayed. Then if no touch is detected within a third predetermined period, control reverts to the Attractor module shown in FIG. 9.

If, at 320, the area labeled "How to use the GCC" is touched, control moves to 322 where a short demonstration of the steps needed to complete the purchase of a gift certificate is shown. At any time during that demonstration a touch on the area of the screen marked "Go Back" will terminate the demonstration display and move control back to 320. In any event, after the demonstration concludes, control moves back to 320.

If, at 320, the area labeled "Browse" is touched, control moves to 324 where an abbreviated step-through of the demonstration of 322 is shown. At any time during the step-through a touch on the area of the screen marked "How to Use the GCC" will terminate the demonstration display and control will move to 322. A touch on the area marked "Select a Store" will move

control to 326. In any event, after the demonstration concludes, control moves back to 320.

At each step of the purchase, a voice message complementary to the screen display guides the customer in the next decision. If, at 320, the area labeled "Start Shopping" is touched, control moves to 326 where a screen is displayed with clearly marked areas labeled "Shop by Store Type", "Shop by Geographic Area", "Shop by List of Stores", "Go Back" and "Help." At the same time, a voice message is broadcast telling the customer the next step in the purchase. The merchant named on the gift certificate can be chosen by category, by geographical locations served or from a list of retailers who serve the local area. The "Go Back" label is provided on a majority of screens to allow users to retrace their steps through the screen displays. The "Help" label is provided to call a series of "Help" screens (not shown) for additional instructions. If an Attractor module is not used, the main program can start at 326.

If, at 326, the area labeled "Shop by Store Type" is touched, control moves to 328 where a screen is displayed with clearly marked areas labeled by category. A touch within one of the marked areas moves control to 330 where a list of stores within that category is displayed. A touch on a retailer from the list of stores in 330 moves control to 332 where short store-specific promotional messages are displayed and broadcasted and then the program moves to 346.

If, at 326, the area labeled "Shop by Geographic Location" is touched, control moves to 334 where a map of the states of the continental United States is displayed. A touch within one of the states moves control to 336 where a graphical representation of the state is displayed with metropolitan areas highlighted. A touch in an area highlighted as a metropolitan area moves control to 338 where a list of

the stores that serve that metropolitan area is displayed. The stores listed may be stores located in that area or stores that provide a mail-order service for that area. The list is displayed such that a touch on touch screen 14 in the vicinity of a retailer on the list selects the retailer and moves control first to 332 where a short store-specific promotional message is displayed and then to 346.

In an alternate embodiment, a list if cities within the state is displayed. A touch of the area around the city name selects the city and moves control to the store list.

If, at 326, the area labeled "Shop by List of Stores" is touched, control moves to 340 where a screen is displayed with list of stores that serve the immediate metropolitan area. When the list is too large to fit on one display screen the consumer can scroll down the list by touching the area marked "Continue List" and moving to 342. At 342, the consumer can also scroll back up the list (and move back to 340) with the "Go Back" command. A touch within the vicinity of one of the stores on the list in either 340 or 342 selects the store. Control moves to 332 for the display of a short promotional message related to the selected store prior to moving to 346.

In an alternate embodiment, a screen display 344 is provided to provide customer feedback. The screen displays of 340 and 342 would include a marked area labeled "Request a Store". A touch in the vicinity of "Request a Store" causes the program to move to 344 where the customer can enter the name of the desired storethrough touch screen 14 using a keyboard displayed on monitor 12.

Once a store has been selected control moves to 346 as shown in FIG. 10b to complete the purchase. At 346 a screen is displayed with clearly marked areas labeled "More about this Store" and "Select a

Certificate". Computer 24 then waits for a selection made by touching within the marked areas on touch screen 14. Selection of the area marked "More about this Store" takes the program to 348 where a longer promotional message related to the selected store is displayed. This message may include information on products and services and on current sales promotions. In the preferred embodiment, on conclusion of the promotional message control moves back to 346.

If, at 346, touch screen 14 is touched in the area marked "Select a Certificate", control moves to 350. At 350 a screen is displayed listing the types of certificates offered by the selected store. In the preferred embodiment, certificates can be issued for goods, services or monetary value. The item chosen is printed as text or as a graphical representation of that item to section 206 of certificate 200 in FIG. 12. Since more than one certificate can be purchased at one time, a separate window is displayed on monitor 12 showing charges accumulated so far in the transaction. The customer chooses the type of certificate desired by touching in the vicinity of a label from a group of labels including monetary values and available goods and services. If the desired monetary values are not displayed, the customer can select the label marked "Another amount not shown". Control then moves to 352 and other values can be selected. Once a value is selected at 350 or 352, control moves to 354 in order to charge the purchase to a credit card.

At 354 a list of accepted credit cards is displayed. The customer selects the form of payment and at 356 computer 24 displays the form of payment selected and the question "Would you like to purchase more than one certificate?". If at 356 the answer is "Yes", the data corresponding to the previous certificate selected is saved and control moves to 350 so that additional

certificates can be purchased. If the answer is "No", control moves to 358.

At 358 a graphic is displayed showing the process of inserting or swiping a credit card. Card reader 16 notifies computer 24 that a card has been swiped and transfers the data encoded in the magnetic strip of the card. Computer 24 then initiates a call to credit authorization computer 62 for card validation as shown in FIG. 8 and explained below. Card validation is required before a certificate can be printed. In the preferred embodiment, card validation is handled as a separate, independent task. If a negative credit report is received from computer 62, at the next screen transition control moves to 354 where a list of forms of payment is again displayed and an opportunity is offered for the use of a different form of payment.

While the call is being made to computer 62, control moves to 360 where a request is displayed for the intended recipient's name. The customer touches "Yes" to indicate a name will be entered and control moves to 362. If "No" is selected control moves to 370 where a personal message can be entered on each certificate.

At 362 as shown in FIG. 10c the customer can enter the name of the intended recipient through touch screen 14 using a keyboard displayed on monitor 12. The typed name is displayed in a graphic of the completed gift certificate while the name is being entered. When the customer is finished entering the name, control moves to 364 where the customer can select a message to be printed on the gift certificate.

In an alternate embodiment, the customer can enter the name and address of the recipient at 362 and an envelope is printed bearing the address of the recipient.

At 364 a screen is displayed providing the opportunity to enter either a prepared message or a

custom greeting. Selection of a prepared message is done by touching in the vicinity of the message displayed. Control then moves to 370. Selection of a custom message is done by touching the "Custom Message" label displayed on the screen of 364.

If a custom message is selected at 364, control moves to 368 where a keyboard is displayed for entering a custom message. When the message is completed control moves to 370 where a representation of certificate 200 is displayed along with the question "Is this correct?" and the labels "Yes" and "No". If the answer is "No" control moves to 372 where certificate 200 is displayed again along with the labels "Amount", "Greeting", "Names" and "Store". If "Amount" is selected control moves to 350 to change the type of certificate. If "Greeting" is selected control moves to 364 to change the message. If "Name" is selected control moves to 360 to change or delete the customer's or the recipient's name.

If, at 370, the certificate is deemed to be completed correctly the customer selects "Yes". If the card validation call has been completed and the charges authorized control moves to 376. If the card validation call has not been completed control moves to 374 and a screen is displayed showing that the credit check is still in progress. Control remains at 374 until the card validation call to computer 62 is completed. When the call is completed, if credit was not authorized, a message to that effect is displayed and control moves 354. If credit was authorized control moves to 376.

If, at 370, the certificate is deemed to be completed correctly the customer selects "Yes" and control moves to 374 where a signature capture routine is called so that the customer can enter a verification signature. Once the signature is completed and the card and charges validated by computer 60 via card authorization computer 62, control moves to 376. If the

card validation call has not been completed control moves to 374 and a screen is displayed showing that the credit check is still in progress. 1485XContremains at 374 until the card validation call to computer 62 is completed. When the call is completed, if credit was not authorized, a message to that effect is displayed and control moves 354. If credit was authorized control moves to 376.

At 376 the gift certificate is displayed and the customer is asked if the certificate should be printed. If the user selects "Print/Purchase", control moves to 378 where a signature capture routine is called so that the customer can enter a verification signature. Once the signature is completed control moves to 380 where an envelope is dispensed and an offer extended to purchase another certificate. If the answer is "Yes" control moves to 326. If "No" control moves to 382 where a brief "thank you" message is displayed before control moves back to 300 of the Attractor module of FIG. 9.

FIG. 11 illustrates the preferred embodiment of the "Browse" routine shown as 324 in FIG. 10a. The "Browse routine is entered at 390 where a series of visuals is displayed of retailer's logos and completed certificates. At 392 a short demonstration of a user purchasing a gift certificate is displayed. At 394 a graphic is displayed of a satisfied customer receiving a certificate. At 396 a statement listing the charges for purchasing a certificate is displayed along with a graphic demonstrating accumulation of charges on the receipt section of a completed gift certificate. And at 398 the customer is invited to create and display (but not print) a sample certificate. Control then moves back to the calling routine.

In a second embodiment of the main program, the screen displayed at 320 in FIG. 10a is modified to offer the customer the option of creating a gift certificate

before committing to a purchase. ("Try Before Buy" vs. "Buy.") This option replaces the "Browse" and "How to Use the GCC" routines of the first embodiment. To clarify this option, a voice message is generated explaining that customers can go through all the steps of creating a gift certificate before they need to insert a credit card to complete the purchase. The selection of "Try" or "Buy" is saved before the routine moves to 320.

From 326, the main program follows the steps of FIGS. 10a and 10b until the routine reaches 358. There, if the "Try" option was chosen, step 358 is skipped and the routine moves directly from 356 to 360. The routine continues to 370. If, at 370, "Yes" is selected, and previously, "Try" was selected, the customer is offered the opportunity to insert a credit card and complete the purchase.

A series of routines used to perform functions within the main program are described next. A system shutdown routine used to secure a gift certificate dispensing device 10 is illustrated in FIG. 6. The routine is entered at 110 where computer 24 initiates display of an "Out of Order" screen on monitor 12. At 112 touch screen 14 is disabled and at 114, a call is placed through modem 42 to main computer 60 to log the reason for system shut down.

A routine used to initiate a call to main computer 60 or credit card authorization computer 62 is shown in FIG. 7. For the sake of brevity the routine will be described for a call to computer 60. It should be obvious to one skilled in the art that this routine can be used to initiate a call to any external computer through modem 42. Also, this routine is used to set up the call; the calling routine takes over communicating to the external computer and terminates the call when ended. The routine is entered at 120 where modem 42 is set to a known condition. At 122 an attempt is made to

access public telecommunications channel 46. At 124 computer 24 checks for a dial tone at modem 42. If a dial tone is not found, at 126 computer 24 increments the retry count, executes a program to wait for five seconds and checks to see at 128 if that was the third time a dial tone was not detected. If so, control moves to 130 and an error status is returned to the calling routine. If not, control moves to 120, modem 42 is again reset and the routine continues.

If a dial tone is found at 124, at 132 computer 24 commands modem 42 to dial computer 60. If at 134 a busy tone is detected, at 136 computer 24 initiates a program to wait five minutes and move to 137. If at 137 it is determined that this is the third failure, control moves to 130 and an error status is returned to the calling routine. If not, control moves to 132 to try the call again. If at 138 there is no answer after a predetermined number of rings or at 140 an off-hook is detected without a carrier, control moves to 136 to wait before trying again.

If a carrier is detected at 140, at 142 a security routine associated with computer 60 is executed. If the proper handshake is not consummated, control moves to 130 and an error status is returned to the calling routine. If security has been verified with the correct handshaking, control moves back to the calling routine to complete the call.

A routine used to validate a credit card swiped through card reader 16 is shown in FIG. 8. This routine is entered at 150 where a call is made to the routine shown in Fig. 7 to initiate the call. The routine shown in FIG. 7 returns with either a normal or an error status. If an error status is returned, at 152 control moves to 154 and an error status is returned to the routine that initiated the credit card validation routine.

If a normal status is returned on call initialization, at 152 control moves to 156 and a credit card validation request is transmitted to computer 62. If at 158, it is determined that the request was not transmitted correctly, at 160 a check is made to see if this is the third failure and, if not, control returns to 156 to try again. If at 160 it is determined that this is the third failure, control returns to 150 to initiate the call again.

If at 158 it is determined that the request was transmitted correctly, at 162 computer 24 waits a predetermined time period for a response. If the response is not received in that period of time at 164 control moves to 150 to initiate the call again.

If at 162 a response is received before expiration of the predetermined time period at 164 control moves to 166 where the response is translated into a format used by the program. At 168 the translated response is checked for validity. If the response is a valid response, control returns to the calling routine. If the response is not valid, control returns to 156 and the request is transmitted again.

A routine used to capture a signature is shown in FIGS. 15a and 15b. In the preferred embodiment of the signature capture routine two signatures are displayed on the screen. The first, the large signature, traces the movement of the finger on the screen. The second, the small signature, is a reduced version of the large signature placed to show the signature as it will be printed to the gift certificate. The routine is entered at 500 where the background of the screen display is drawn. At 502, touchscreen 14 is initialized, at 504, a signature buffer cleared and, at 506, a timeout count variable is set to zero.

At 508, a check is made for a touch and if a touch is present, at 510 the program moves to 512 to increment the timeout count variable. At 514, a check

is made to see if a predetermined timeout count has been reached. If not, control moves to 508 to check for a touch. If, at 514, it is determined that the predetermined timeout count has been reached, at 516, a flag is set to tell the main program to start over and control is returned to the main program.

If at 508 the check for touch determines a touch is present, at 518 a check is made to see if the touch is in the area of the touchscreen defined for user selection of the option to reenter the signature. If so, control moves to 504 where the signature buffer is cleared.

If at 518 it is determined that the touch was not in the area used to define the reenter signature function, at 520 a check is made to see if the touch is in the area of the touchscreen defined indicating the signature is complete. In the preferred embodiment, the signature is not considered to be complete until the customer indicates that by touching inside the area defined for indicating the signature is complete.

If at 520 it is determined that no touch occurred in the signature area, control moves to 524 where a determination is made as to whether there had been a break in the touching of touchscreen 14. If at 524 it is determined that there has been a break then control moves to 526 where the present touch is saved as the start of a new line segment and control then moves to 506.

If at 524 it is determined that no break occurred in contact of touchscreen 14, control moves to 528 where a line is drawn on monitor 12 from the previous touch point to the present touch point. Control then moves to 530 where a second line is drawn on monitor 12 from the point associated with the previous touch point to a point associated with the present touch point. The endpoints of the small

signature line segments are chosen to scale the large signature line segment by a predetermined scale factor.

Once the line segment associated with the small signature is drawn at 530, control moves to 532 where the line pixels of the large signature line segment are converted to PCX format and saved to the signature buffer before control moves to 504.

In a second embodiment of the signature capture routine, a curve fitting algorithm could be used on the line segments to provide a smoother representation of the signature.

To use the present invention, the customer walks up to gift certificate dispensing device 10 and touches touch screen 14. The customer then selects a store from a list of local merchants or obtains a different list of merchants sorted by category or geographical area served. The customer next enters the type of credit card that will be used to purchase the gift certificate and swipes that card through card reader 16. While gift certificate dispensing device 10 is obtaining credit card authorization, the customer enters the name of the recipient of the card and chooses a personal message.

An image of the certificate with the name of the recipient and the personal message included is displayed for verification. If the certificate looks right the customer initiates printing of the certificate and, if the credit purchase was authorized, a gift certificate 200 is printed and dispensed through slot 18. At the same time an envelope is dispensed through slot 20.

The customer detaches section 202 from certificate 200 as a receipt for his records. The remaining certificate is folded at the intersection of sections 204 and 206, inserted in the envelope and mailed or given to the intended recipient. The charges detailed in section 202 are applied against the

customer's charge account and appear sometime later in a normal credit card billing statement.

Although the present invention has been described with reference to the preferred embodiments, those skilled in the art will recognize that changes may be made in form and detail without departing from the spirit and scope of the invention.

What is claimed is:

1. An electronic certificate dispenser for printing and dispensing a certificate, said dispenser being responsive to a user wielding a planar card having magnetic coded data disposed thereon, said dispenser comprising:

a housing;

a card reader for reading magnetic coded data disposed on said planar card and for providing a first output signal representative of said coded data, said reader being supported by said housing;

certificate dispensing means supported by said housing for dispensing certificates, said dispenser means including printing means for printing one or more messages as specified by the user on one of said certificates; and

control means under user control connected to said card reader and said dispensing means for receiving and verifying said first output signal and controlling the printing and dispensing of certificates from said dispensing means.

2. The electronic certificate dispenser of claim 1 wherein the control means includes a programmable first computer, connected to said card reader and said printing means, for verifying under program control the coded data received from said card reader and for controlling and monitoring the printing and dispensing of certificates from said dispenser means.

3. The electronic certificate dispenser of claim 1 wherein said control means includes user interface means for user selection of options in certificate printing and dispensing.

4. The electronic certificate dispenser of claim 2 wherein the control means further includes a second

computer and communication means connected to said programmable first computer for communicating with said second computer in order to verify said coded data.

5. The electronic certificate dispenser of claim 2 wherein the control means includes nonvolatile data storage means connected to said programmable first computer for storing graphics to be printed on said certificates under user control.

6. The electronic certificate dispenser of claim 3 wherein said user interface means includes a monitor and touch screen mounted on said monitor for selecting from options displayed on the monitor.

7. The electronic certificate dispenser of claim 1 wherein the electronic certificate dispenser further comprises envelope dispenser means connected to said control means for dispensing envelopes for said certificates.

8. An electronic certificate dispenser for printing and dispensing a certificate, said dispenser being responsive to a user wielding a planar credit card having magnetic coded data disposed thereon, said dispenser comprising:

a certificate having a plurality of sections with a series of perforations marking an intersection of a pair of said sections, said certificate comprising a material and a first of said sections including a holographic foil mounted on said material;

a card reader for reading said magnetic coded data disposed on said planar credit card and for providing a first output signal;

certificate dispensing means for dispensing said certificate, said dispensing means including

printing means for printing one or more messages on said certificate;

a programmable computer under user control connected to said card reader and said dispensing means, said computer including program means for reading said first output signal and allowing said user to print and dispense said certificate;

wherein said first section is a certificate for subsequent commercial usage and a second of said sections is a user receipt, said holographic foil making thievery less likely.

9. The electronic certificate dispenser of claim 8 wherein said first section still further includes a unique identifying code.

10. An electronic certificate dispenser for printing and dispensing a certificate and for dispensing an envelope, said dispenser being responsive to a user wielding a planar card having magnetic coded data disposed thereon, said dispenser comprising:

a housing having a plurality of vertical panel-like wall portions;

a card reader for reading the magnetic coded data disposed on said planar card and for providing a first output signal representative of said coded data, said reader being supported by said housing and including receiving means in a first of said vertical panel-like wall portions for receiving said planar card;

certificate dispensing means for dispensing certificates and envelope dispensing means for dispensing envelopes, said certificate and said envelope dispensing means being supported by said housing with said certificate dispensing means having first delivery means in another of said vertical panel-like wall portions other than said first for delivering a specific certificate and said envelope dispensing means having

second delivery means in another of said vertical panel-like wall portions other than said first for delivering a specific envelope; and

control means connected to said card reader and said certificate and envelope dispensing means for receiving and verifying said first output signal and controlling the printing and dispensing of certificates and envelopes;

wherein said user can stand in front of the first vertical panel-like wall portion to use said card reader and said control means and can then move away from said first vertical panel-like wall portion to near said appropriate another vertical panel-like wall portions to receive said specific certificate and envelope.

11. A gift certificate purchasing and dispensing system enabled by a credit card and allowed to complete a transaction on validation from a credit card verifying and credit limit checking system, comprising:

a plurality of terminal means including means for allowing a customer to choose a gift certificate and to authorize a debit to a credit card account, each of said terminal means including means for accessing said credit card verifying and credit limit checking system, each of said terminal means also including means for dispensing said gift certificate;

central processing unit means for communicating with said plurality of terminal means and processing data on said gift certificates and said debits to credit card accounts; and

debiting means for debiting said debits to said credit card accounts.

12. The gift certificate purchasing and dispensing system of claim 13 including notifying means for

notifying merchants regarding gift certificates purchased.

13. A method of printing, under user control, from an electronic certificate dispenser, certificates to be used for obtaining goods or services, wherein said electronic certificate dispenser includes display means, card reader means and user interface means, said method comprising:

displaying on said display means a menu of goods and services;

interacting by said user with said user interface means to choose one of said goods and services;

displaying on said display means a menu of of retailers of goods and services;

interacting by said user with said user interface means to choose one of said retailers;

displaying on said display means a series of monetary values;

interacting by said user with said user interface means to choose one of said monetary values;

monitoring the card reader means for the presence of a planar card having magnetic data disposed thereon;

reading said magnetic data with said card reader means;

verifying said planar card is usable for enabling issuance of a certificate;

receiving from said user interface means the retailer and the goods and services chosen;

printing a certificate including the name of the retailer and the goods and services chosen; and

dispensing said certificate.

14. The method according to claim 13 wherein the method further comprises dispensing an envelope for said certificate.

15. A method of printing, in association with a programmable computer and in response to the insertion of a planar card including magnetic coded data disposed thereon, a gift certificate for use in purchasing goods or services, wherein said coded data includes an account name and an account number, comprising:

providing a blank certificate, wherein said certificate includes a plurality of sections with a series of perforations marking an intersection of the sections;

choosing the name of a purveyor of goods and services and a monetary value for the gift certificate;

printing within a first section of said certificate the name of the purveyor, and the monetary value chosen; and

printing within a second section of said certificate a receipt including account name, account number and cost of975Xthansaction, the cost being an incremental amount greater than the value of the certificate.

16. The method according to claim 15 including the step of choosing an item and the step of printing includes printing a representation of the item on the first section of the certificate.

17. The method according to claim 16 wherein the step of printing a certificate includes causing said dispenser to retrieve from said computer and print graphics representative of the purveyor chosen on both the first and second sections of the certificate.

18. The method according to claim 15 wherein the method further comprises:

providing the name of the intended recipient; and

printing within said first section the name of the intended recipient.

19. The method according to claim 18 wherein the method further comprises:

providing a personal message; and

printing within a third section the name of the intended recipient and the personal message.

20. The method according to claim 15 wherein the method further comprises limiting choice of a certificate value to a maximum amount.

21. The method according to claim 15 wherein the method further comprises:

retrieving from said computer a control serial number; and

printing within the first section the control serial number.

22. A method of purchasing and dispensing gift certificates from a dispensing system including a plurality of terminal means and central processing unit means, whenever a credit card verifying and credit limit checking system validates a credit card account and its credit limit, comprising the steps of:

receiving a choice of a name of a purveyor of goods and services and a value for a gift certificate;

receiving a credit card and accessing said credit card verifying and credit limit checking system;

dispensing said gift certificate for said purveyor and said value;

communicating data on said gift certificate and an associated debit to a credit card account based on the value of said gift certificate from said terminal means to said central processing unit means; and

debiting said debit to said credit card account based on data collated by said central processing unit from all terminal means.

23. The method according to claim 22 wherein the method further comprises notifying said purveyors regarding gift certificates purchased.

24. A monetarily-valuable, exchange certificate, comprising:

a sheet of material with printing thereon, said printing including information providing an exchange value for said certificate;

a holographic foil;

means for affixing said foil to said sheet;

wherein said foil would be extremely difficult to copy thereby making said certificate difficult to counterfeit.

25. A user-activated system for creating a monetarily-valuable, exchange certificate, comprising:

a sheet having a plurality of sections with a series of perforations marking an intersection of adjacent said sections, a first of said sections being preprinted; and

means, under control of said user, for receiving said certificate and printing on a second of said sections a value selected by said user indicating worth of said second section in full exchange for a second good or service.

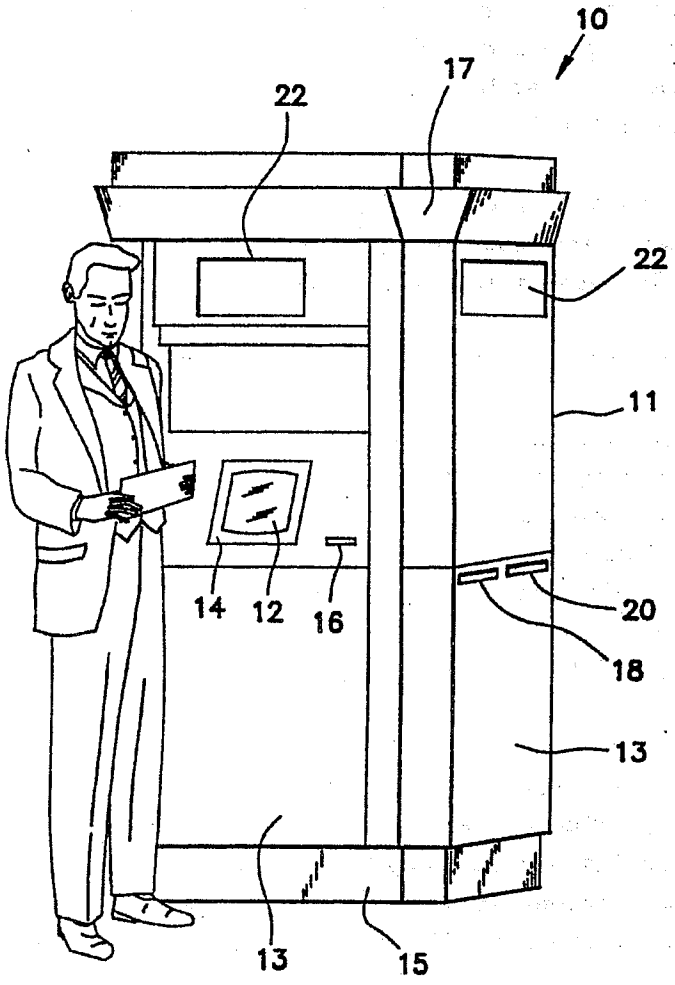


FIG. 1

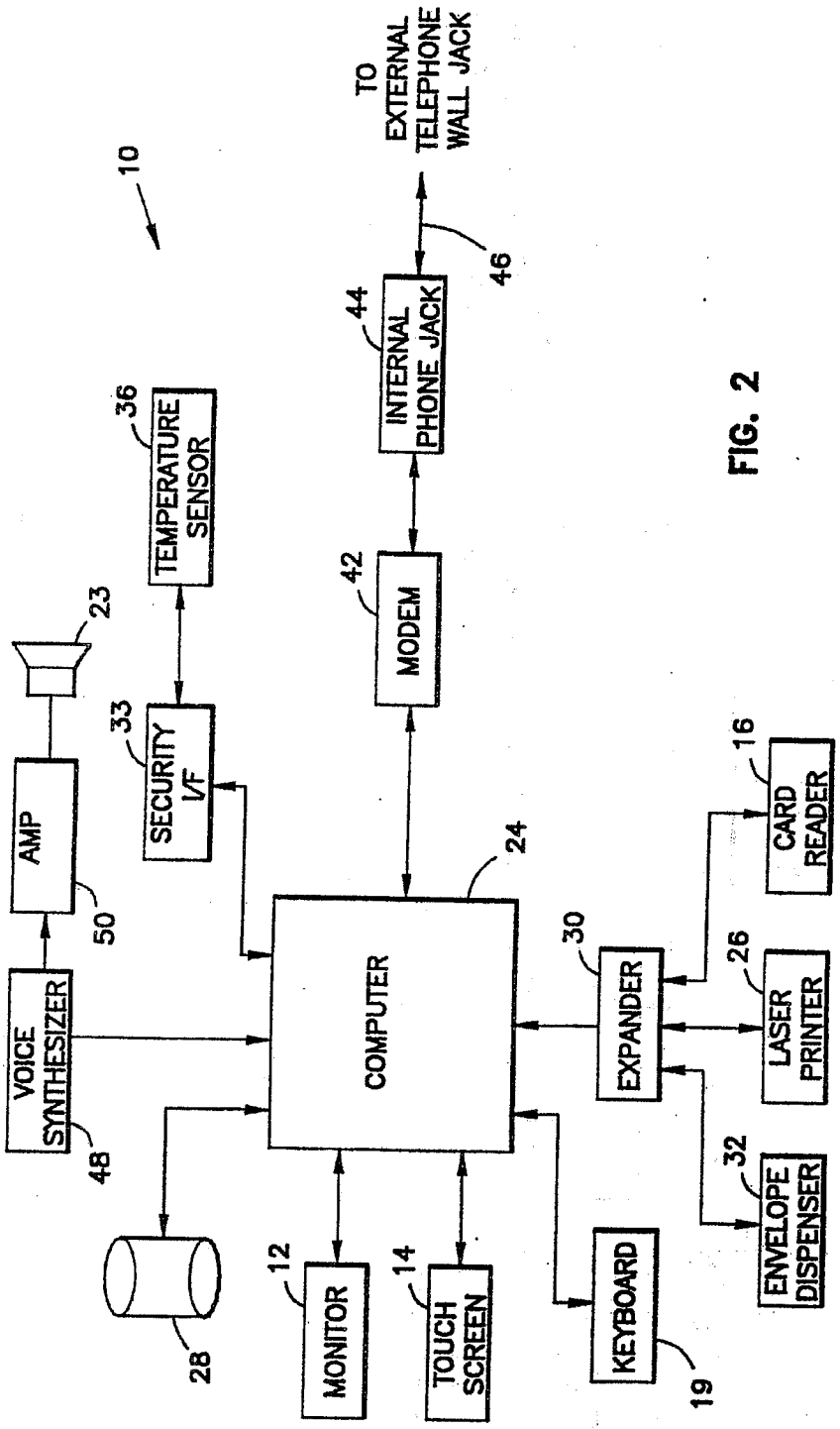

10
TO EXTERNAL TELEPHONE WALL JACK
46
44
INTERNAL PHONE JACK
42
MODEM
36
TEMPERATURE SENSOR
23
33
SECURITY I/F
AMP
50
VOICE SYNTHESIZER
48
COMPUTER
24
16
CARD READER
30
EXPANDER
26
LASER PRINTER
32
ENVELOPE DISPENSER
KEYBOARD
19
12
MONITOR
14
TOUCH SCREEN
28

FIG. 2

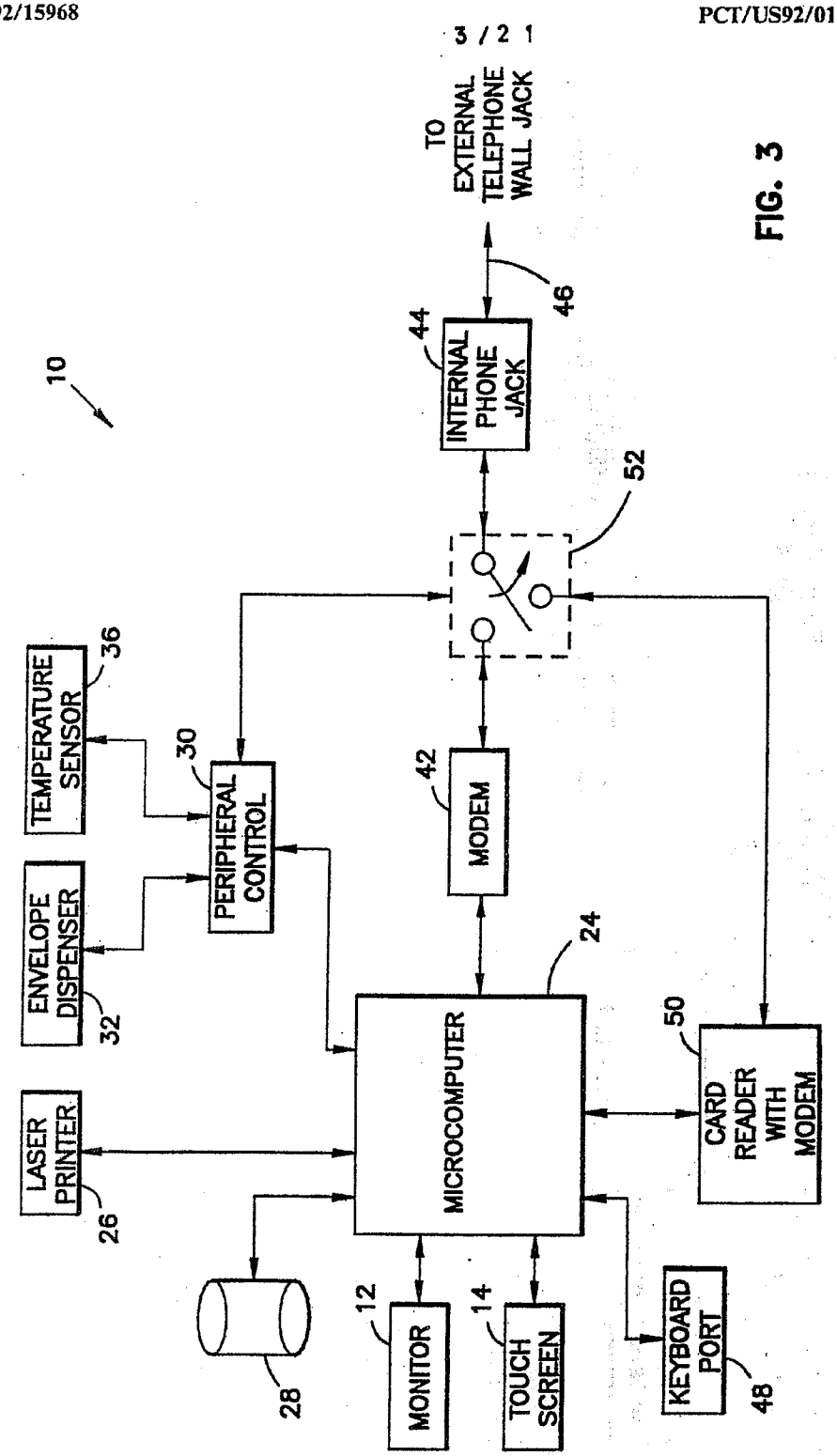

10
TO EXTERNAL TELEPHONE WALL JACK
46
44
INTERNAL PHONE JACK
52
36
TEMPERATURE SENSOR
30
PERIPHERAL CONTROL
42
MODEM
ENVELOPE DISPENSER
32
24
MICROCOMPUTER
50
CARD READER WITH MODEM
LASER PRINTER
26
28
12
MONITOR
14
TOUCH SCREEN
KEYBOARD PORT
48

FIG. 3

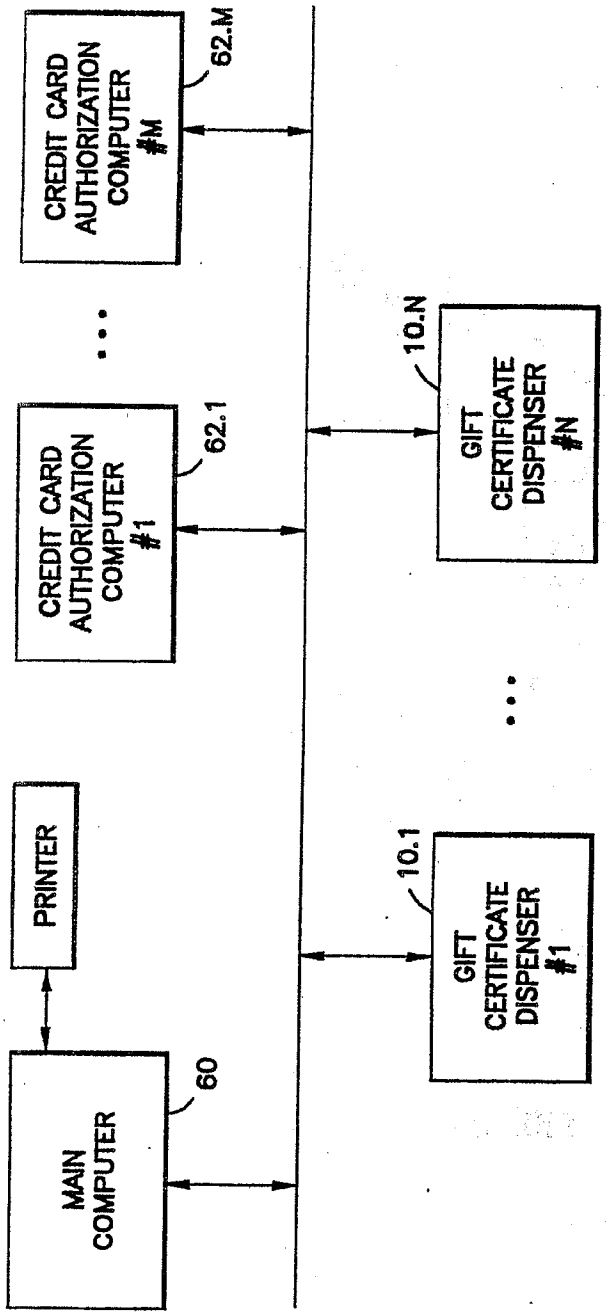

CREDIT CARD AUTHORIZATION COMPUTER #M
62.M
CREDIT CARD AUTHORIZATION COMPUTER #1
62.1
GIFT CERTIFICATE DISPENSER #N
10.N
GIFT CERTIFICATE DISPENSER #1
10.1
PRINTER
MAIN COMPUTER
60

FIG. 4

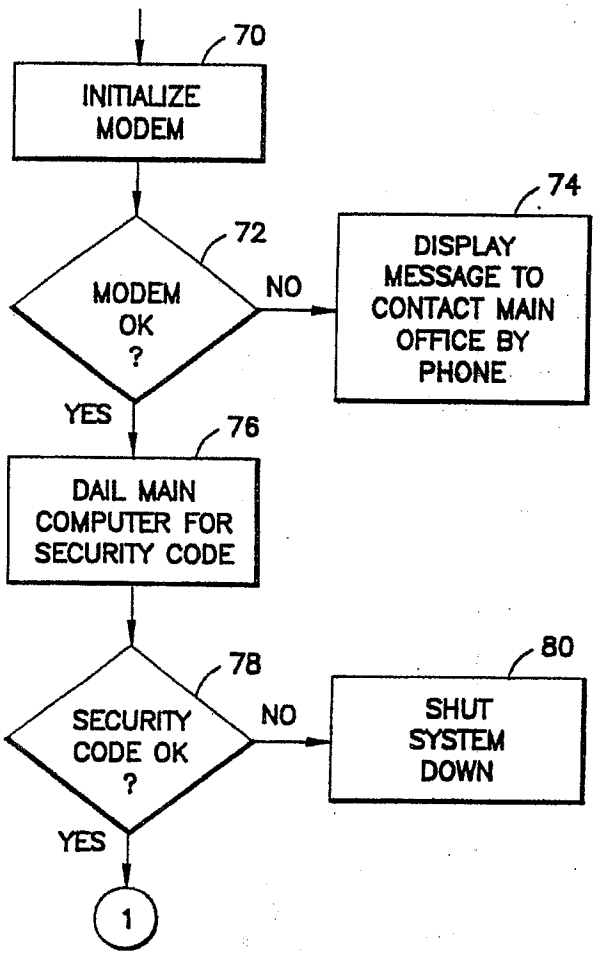

70
INITIALIZE MODEM
72
MODEM OK ?
NO
74
DISPLAY MESSAGE TO CONTACT MAIN OFFICE BY PHONE
YES
76
DAIL MAIN COMPUTER FOR SECURITY CODE
78
SECURITY CODE OK ?
NO
80
SHUT SYSTEM DOWN
YES
1

FIG. 5A

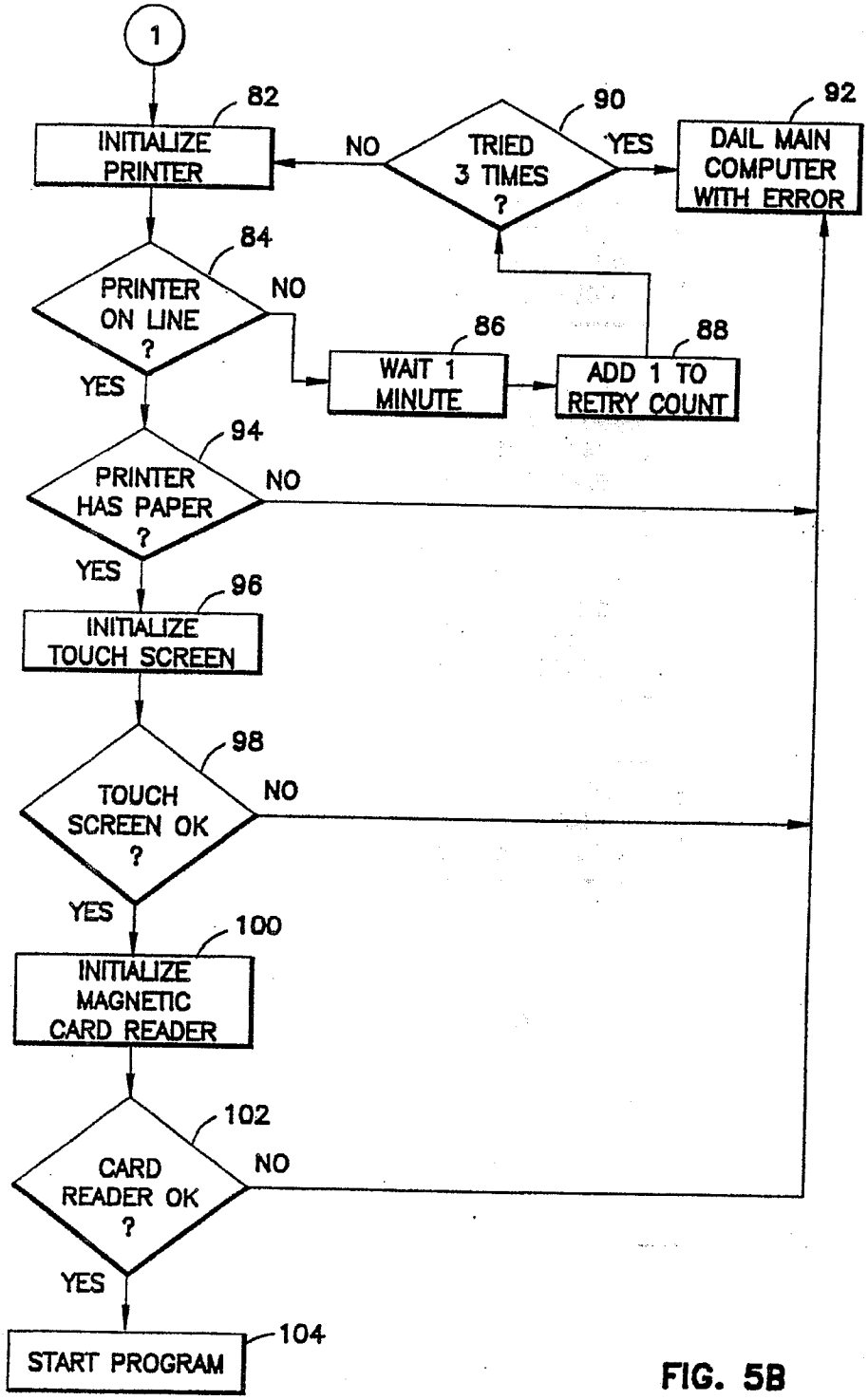

1
82
INITIALIZE PRINTER
NO
90
TRIED 3 TIMES ?
YES
92
DAIL MAIN COMPUTER WITH ERROR
84
PRINTER ON LINE ?
NO
86
WAIT 1 MINUTE
88
ADD 1 TO RETRY COUNT
YES
94
PRINTER HAS PAPER ?
NO
YES
96
INITIALIZE TOUCH SCREEN
98
TOUCH SCREEN OK ?
NO
YES
100
INITIALIZE MAGNETIC CARD READER
102
CARD READER OK ?
NO
YES
104
START PROGRAM

FIG. 5B

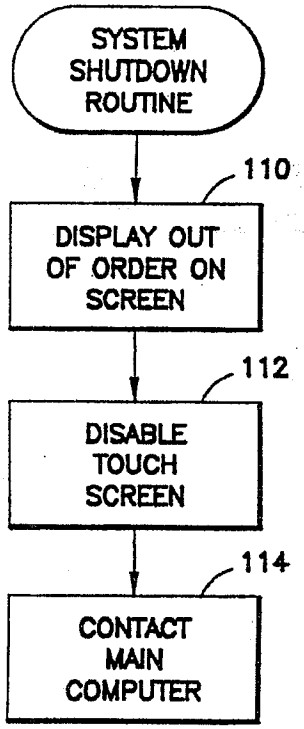

SYSTEM SHUTDOWN ROUTINE
110
DISPLAY OUT OF ORDER ON SCREEN
112
DISABLE TOUCH SCREEN
114
CONTACT MAIN COMPUTER

FIG. 6

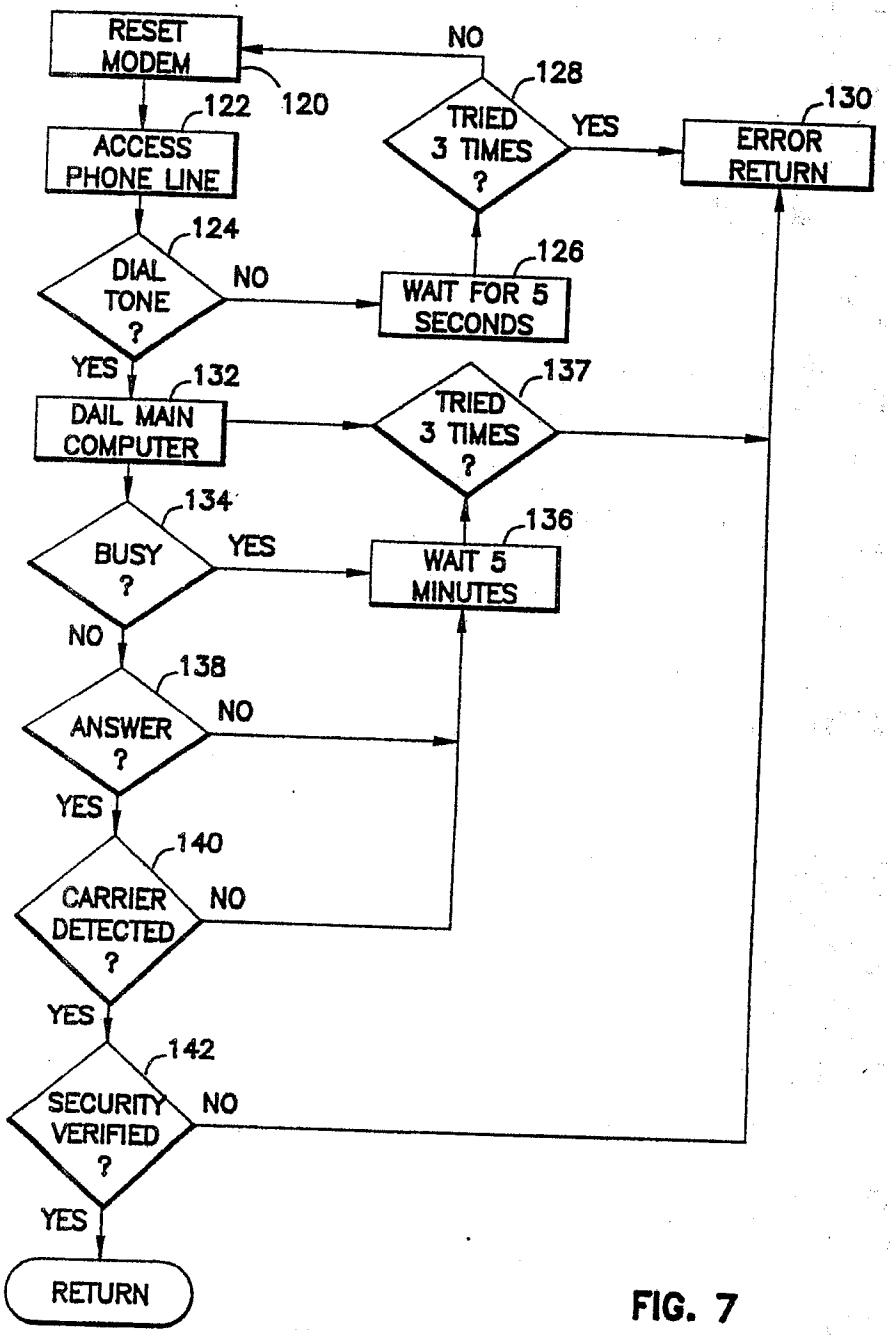

RESET MODEM
120
122
ACCESS PHONE LINE
124
DIAL TONE ?
NO
YES
126
WAIT FOR 5 SECONDS
128
TRIED 3 TIMES ?
NO
YES
130
ERROR RETURN
132
DAIL MAIN COMPUTER
134
BUSY ?
YES
NO
136
WAIT 5 MINUTES
137
TRIED 3 TIMES ?
138
ANSWER ?
NO
YES
140
CARRIER DETECTED ?
NO
YES
142
SECURITY VERIFIED ?
NO
YES
RETURN

FIG. 7

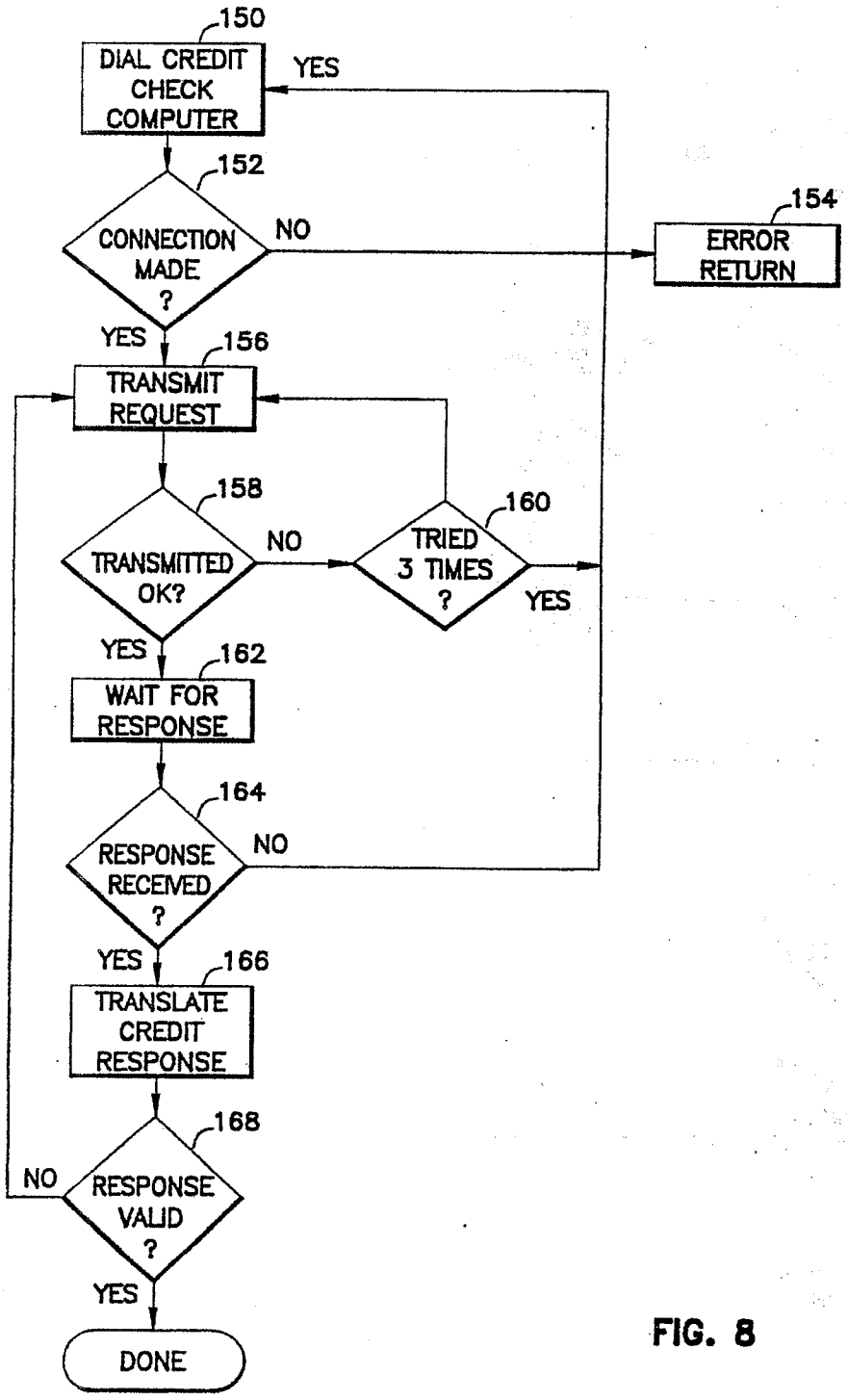

150
DIAL CREDIT CHECK COMPUTER
YES
152
CONNECTION MADE ?
NO
154
ERROR RETURN
YES
156
TRANSMIT REQUEST
158
TRANSMITTED OK?
NO
160
TRIED 3 TIMES ?
YES
YES
162
WAIT FOR RESPONSE
164
RESPONSE RECEIVED ?
NO
YES
166
TRANSLATE CREDIT RESPONSE
168
RESPONSE VALID ?
NO
YES
DONE

FIG. 8

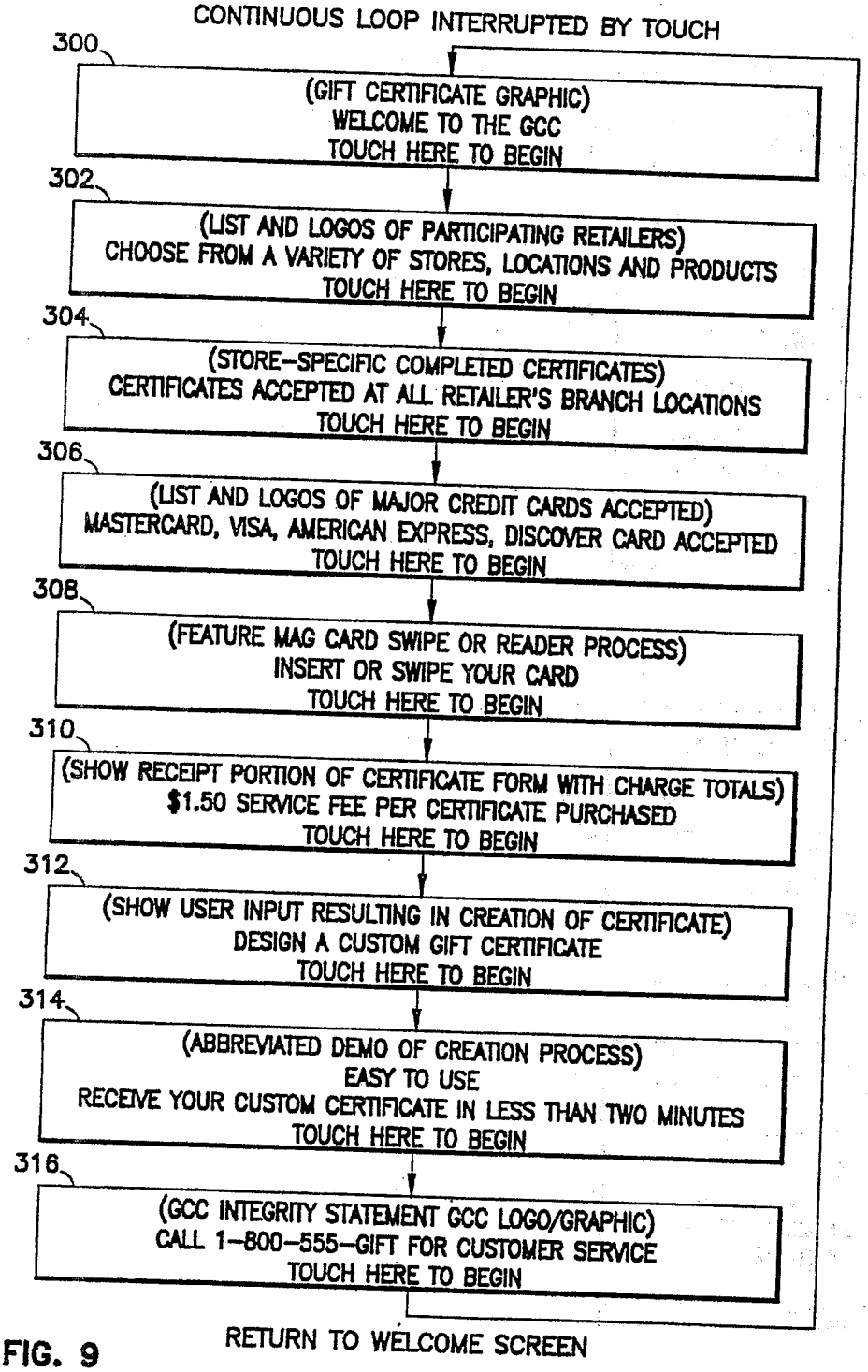

CONTINUOUS LOOP INTERRUPTED BY TOUCH
300
(GIFT CERTIFICATE GRAPHIC)
WELCOME TO THE GCC
TOUCH HERE TO BEGIN
302
(LIST AND LOGOS OF PARTICIPATING RETAILERS)
CHOOSE FROM A VARIETY OF STORES, LOCATIONS AND PRODUCTS
TOUCH HERE TO BEGIN
304
(STORE-SPECIFIC COMPLETED CERTIFICATES)
CERTIFICATES ACCEPTED AT ALL RETAILER'S BRANCH LOCATIONS
TOUCH HERE TO BEGIN
306
(LIST AND LOGOS OF MAJOR CREDIT CARDS ACCEPTED)
MASTERCARD, VISA, AMERICAN EXPRESS, DISCOVER CARD ACCEPTED
TOUCH HERE TO BEGIN
308
(FEATURE MAG CARD SWIPE OR READER PROCESS)
INSERT OR SWIPE YOUR CARD
TOUCH HERE TO BEGIN
310
(SHOW RECEIPT PORTION OF CERTIFICATE FORM WITH CHARGE TOTALS)
$1.50 SERVICE FEE PER CERTIFICATE PURCHASED
TOUCH HERE TO BEGIN
312
(SHOW USER INPUT RESULTING IN CREATION OF CERTIFICATE)
DESIGN A CUSTOM GIFT CERTIFICATE
TOUCH HERE TO BEGIN
314
(ABBREVIATED DEMO OF CREATION PROCESS)
EASY TO USE
RECEIVE YOUR CUSTOM CERTIFICATE IN LESS THAN TWO MINUTES
TOUCH HERE TO BEGIN
316
(GCC INTEGRITY STATEMENT GCC LOGO/GRAPHIC)
CALL 1-800-555-GIFT FOR CUSTOMER SERVICE
TOUCH HERE TO BEGIN
RETURN TO WELCOME SCREEN

FIG. 9

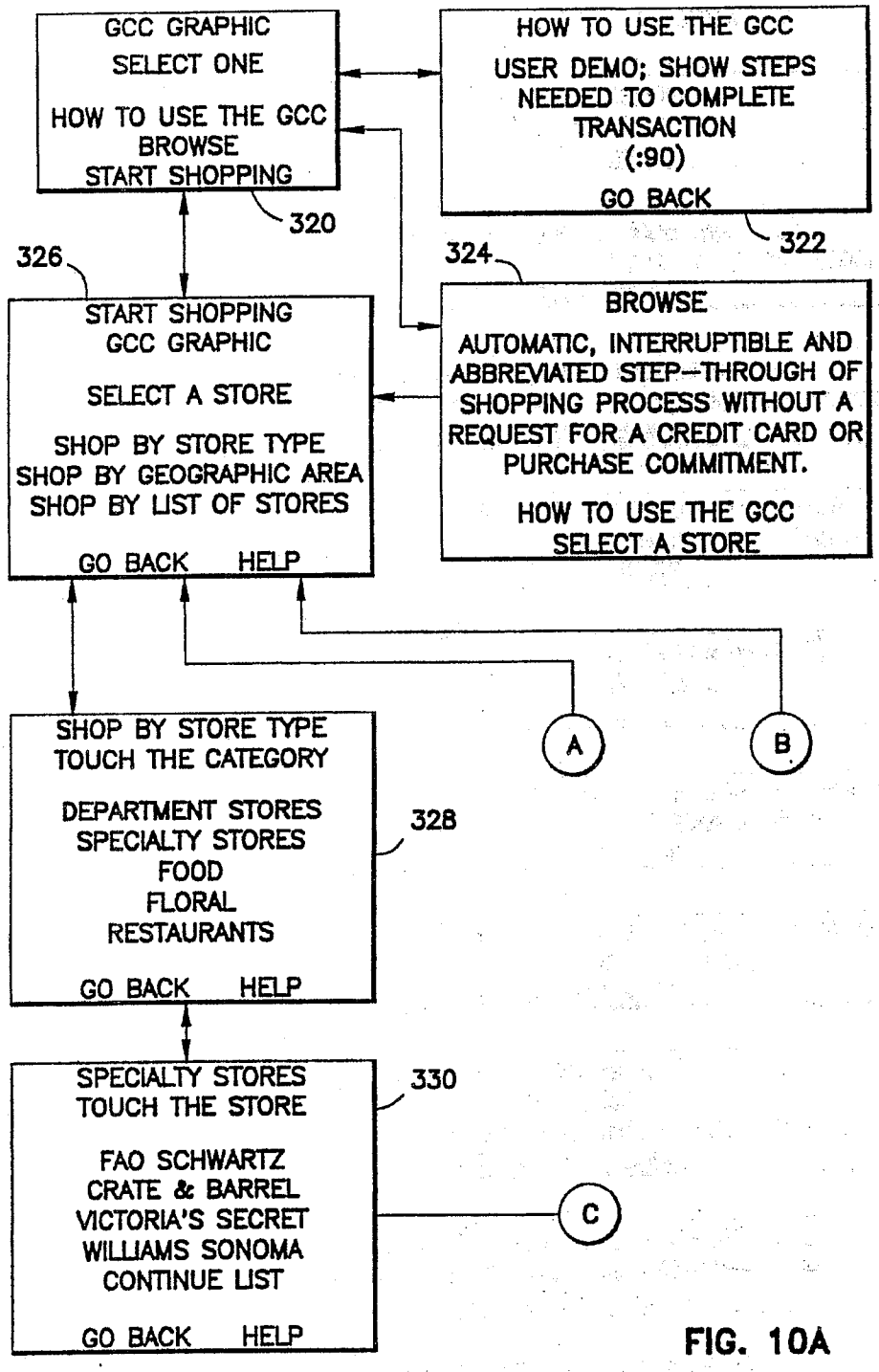

GCC GRAPHIC
SELECT ONE
HOW TO USE THE GCC
BROWSE
START SHOPPING
320
HOW TO USE THE GCC
USER DEMO; SHOW STEPS NEEDED TO COMPLETE TRANSACTION
(:90)
GO BACK
322
326
324
START SHOPPING
GCC GRAPHIC
SELECT A STORE
SHOP BY STORE TYPE
SHOP BY GEOGRAPHIC AREA
SHOP BY LIST OF STORES
GO BACK HELP
BROWSE
AUTOMATIC, INTERRUPTIBLE AND ABBREVIATED STEP-THROUGH OF SHOPPING PROCESS WITHOUT A REQUEST FOR A CREDIT CARD OR PURCHASE COMMITMENT.
HOW TO USE THE GCC
SELECT A STORE
A
B
SHOP BY STORE TYPE
TOUCH THE CATEGORY
DEPARTMENT STORES
SPECIALTY STORES
FOOD
FLORAL
RESTAURANTS
GO BACK HELP
328
SPECIALTY STORES
TOUCH THE STORE
FAO SCHWARTZ
CRATE & BARREL
VICTORIA'S SECRET
WILLIAMS SONOMA
CONTINUE LIST
GO BACK HELP
330
C

FIG. 10A

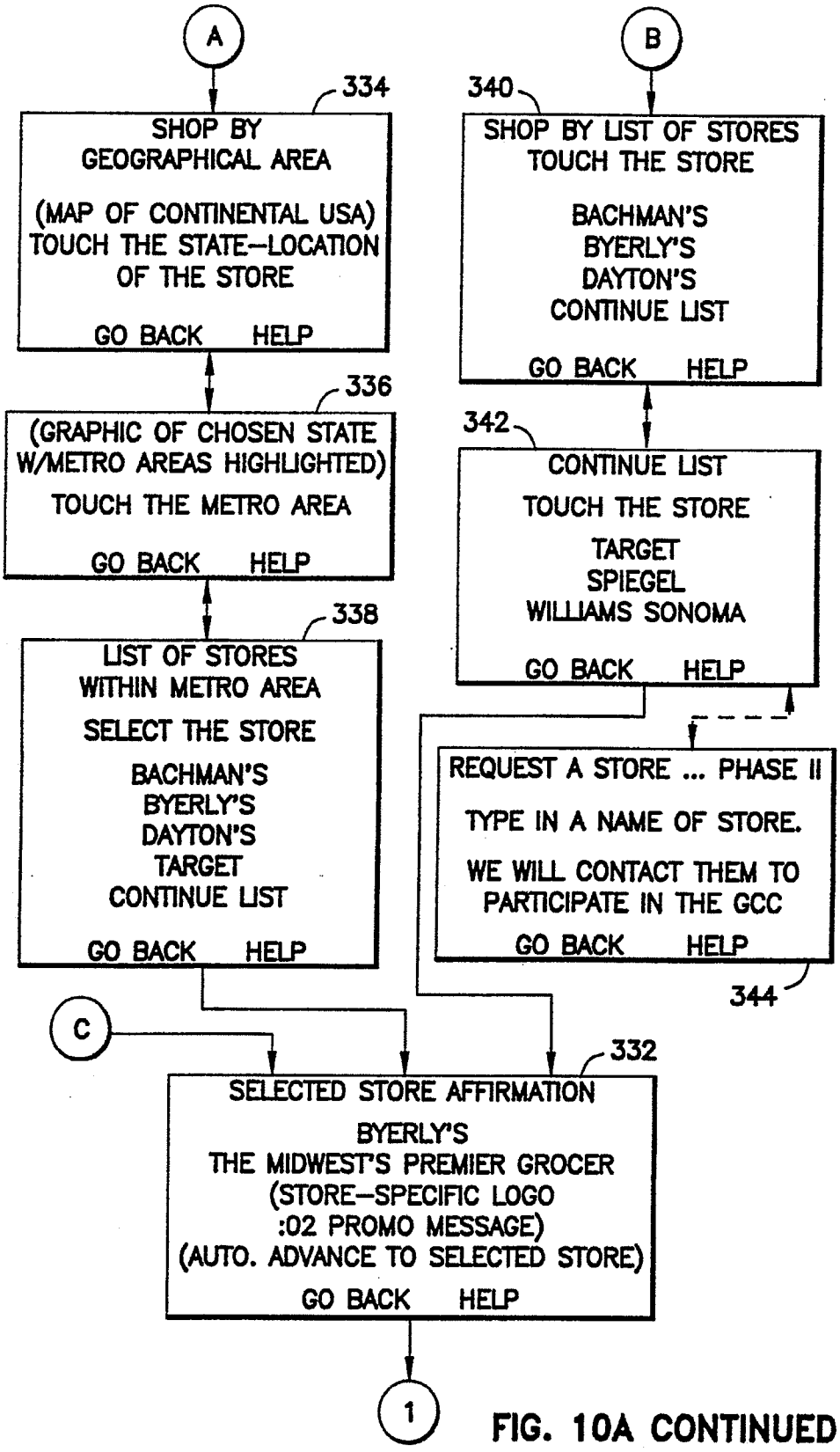


FIG. 10A CONTINUED

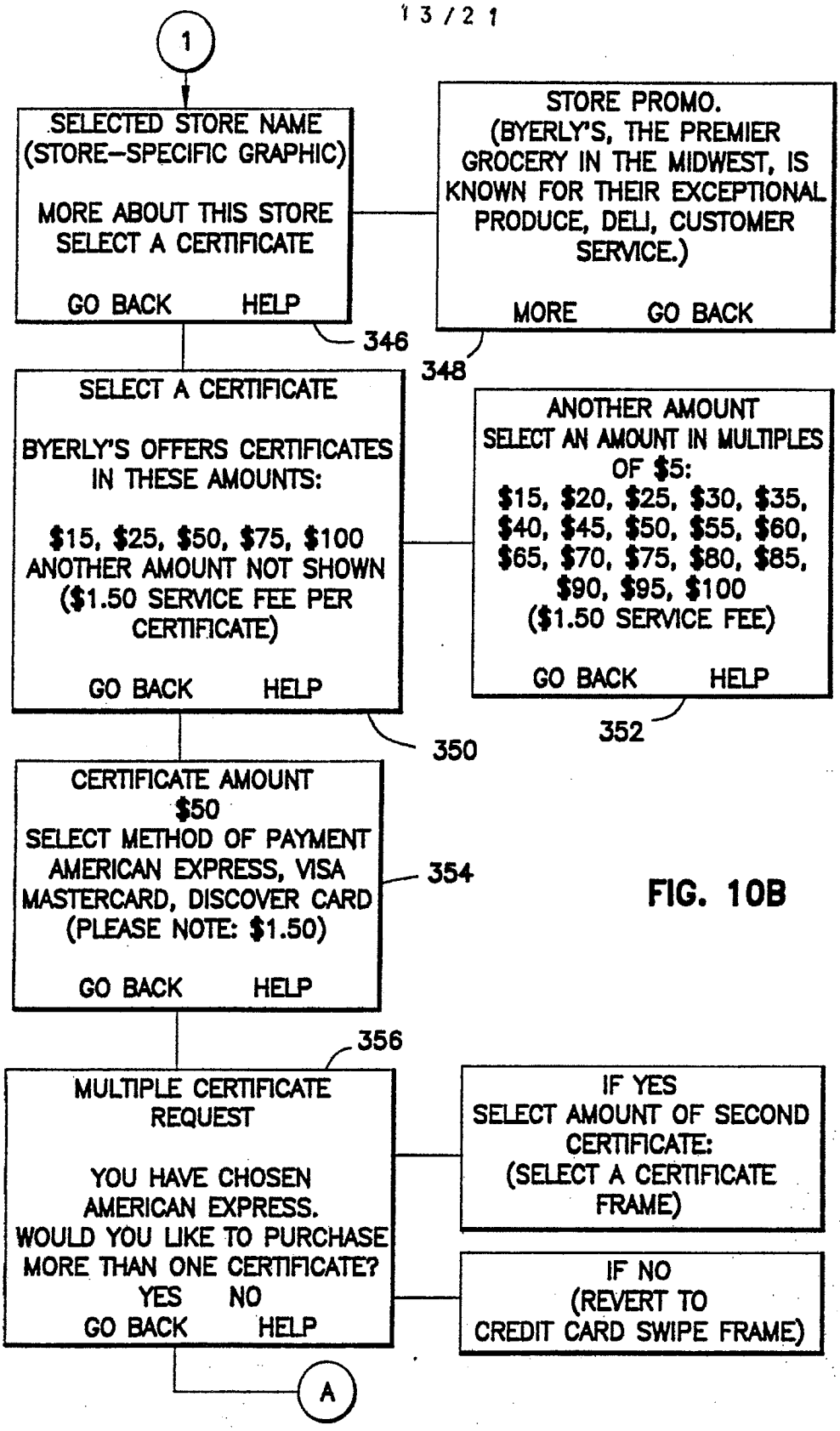

1
SELECTED STORE NAME
(STORE-SPECIFIC GRAPHIC)
MORE ABOUT THIS STORE
SELECT A CERTIFICATE
GO BACK HELP
346
STORE PROMO.
(BYERLY'S, THE PREMIER GROCERY IN THE MIDWEST, IS KNOWN FOR THEIR EXCEPTIONAL PRODUCE, DELI, CUSTOMER SERVICE.)
MORE GO BACK
348
SELECT A CERTIFICATE
BYERLY'S OFFERS CERTIFICATES IN THESE AMOUNTS:
$15, $25, $50, $75, $100
ANOTHER AMOUNT NOT SHOWN
($1.50 SERVICE FEE PER CERTIFICATE)
GO BACK HELP
350
ANOTHER AMOUNT
SELECT AN AMOUNT IN MULTIPLES OF $5:
$15, $20, $25, $30, $35, $40, $45, $50, $55, $60, $65, $70, $75, $80, $85, $90, $95, $100
($1.50 SERVICE FEE)
GO BACK HELP
352
CERTIFICATE AMOUNT
$50
SELECT METHOD OF PAYMENT
AMERICAN EXPRESS, VISA MASTERCARD, DISCOVER CARD
(PLEASE NOTE: $1.50)
GO BACK HELP
354
356
MULTIPLE CERTIFICATE REQUEST
YOU HAVE CHOSEN AMERICAN EXPRESS.
WOULD YOU LIKE TO PURCHASE MORE THAN ONE CERTIFICATE?
YES NO
GO BACK HELP
IF YES
SELECT AMOUNT OF SECOND CERTIFICATE:
(SELECT A CERTIFICATE FRAME)
IF NO
(REVERT TO CREDIT CARD SWIPE FRAME)
A

FIG. 10B

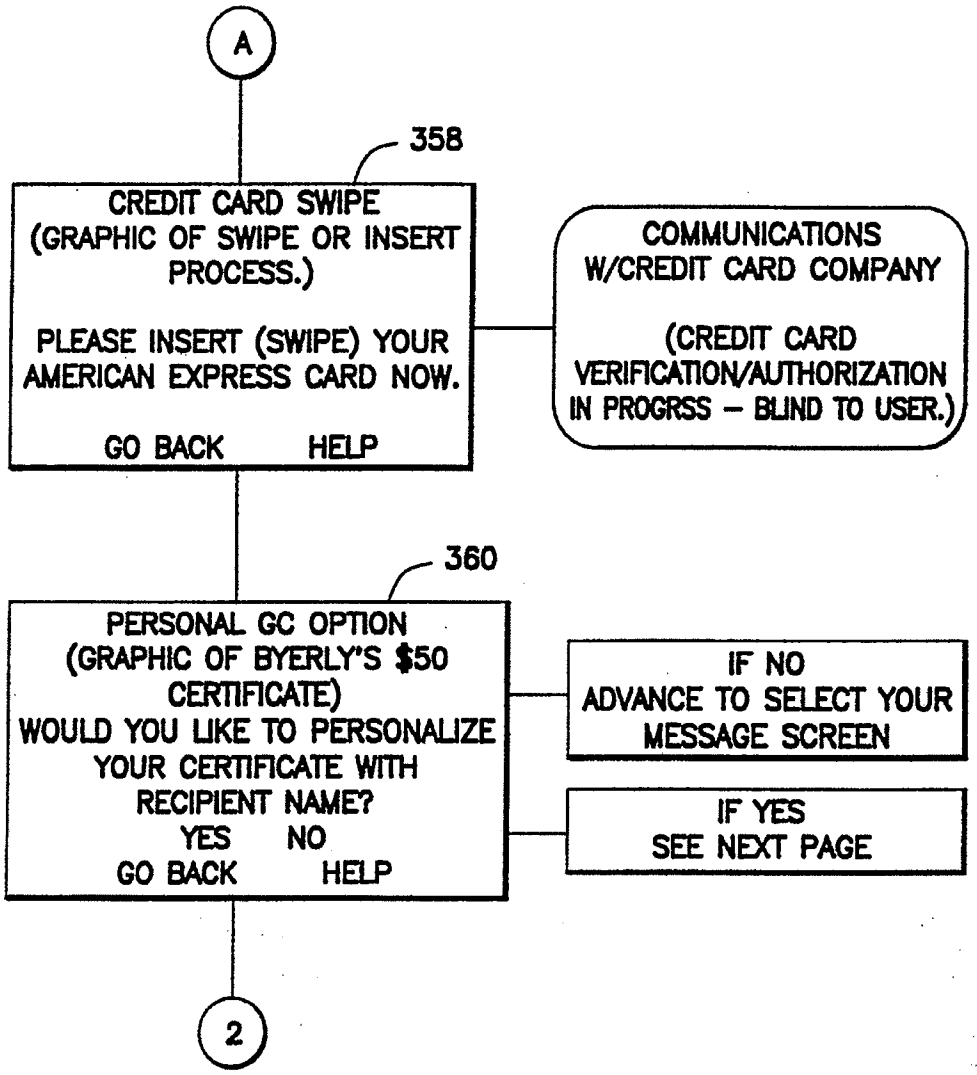


FIG. 10B CONTINUED

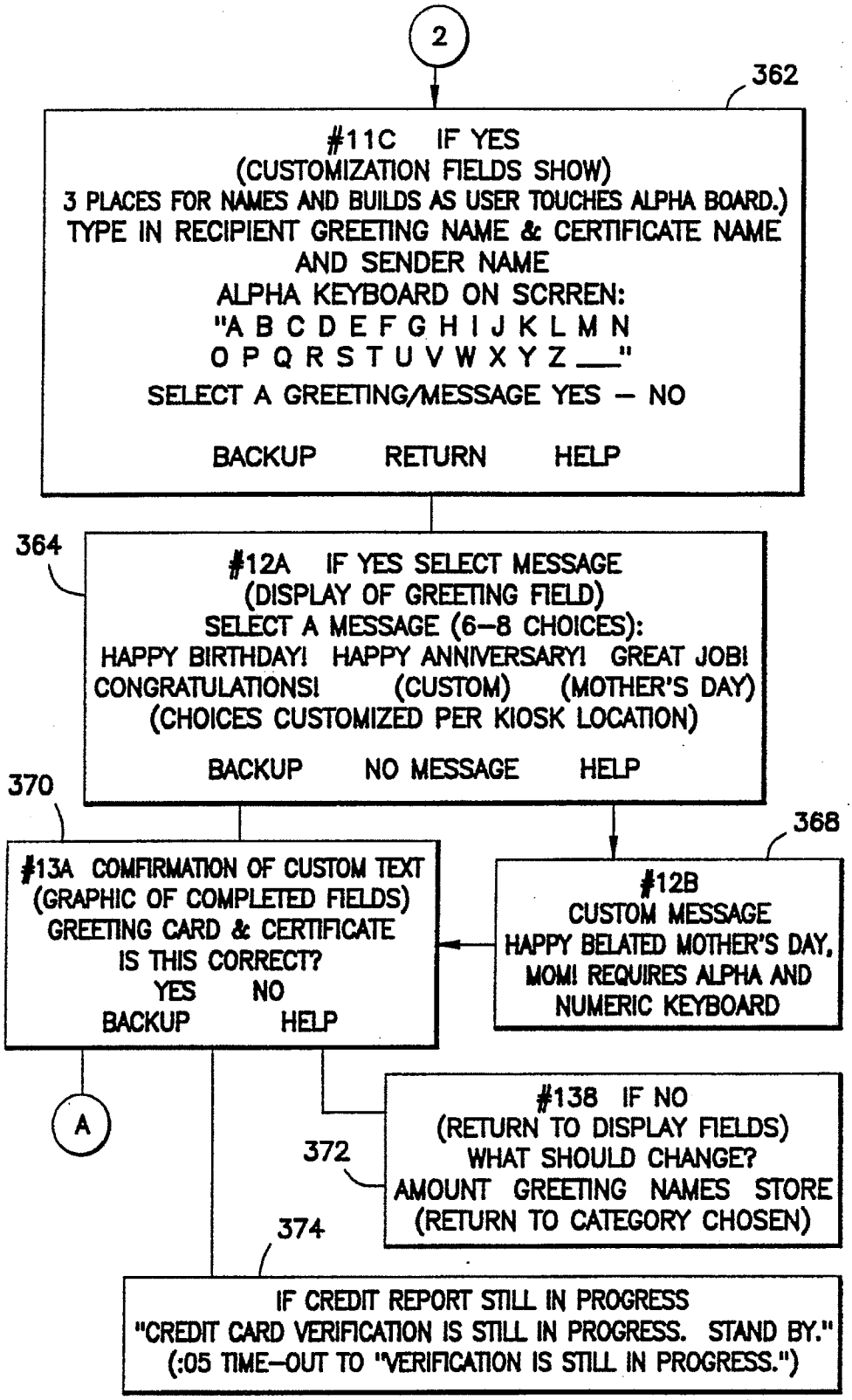

2
362
#11C IF YES
(CUSTOMIZATION FIELDS SHOW)
3 PLACES FOR NAMES AND BUILDS AS USER TOUCHES ALPHA BOARD.)
TYPE IN RECIPIENT GREETING NAME & CERTIFICATE NAME
AND SENDER NAME
ALPHA KEYBOARD ON SCRREN:
"A B C D E F G H I J K L M N
O P Q R S T U V W X Y Z ___"
SELECT A GREETING/MESSAGE YES – NO
BACKUP RETURN HELP
364
#12A IF YES SELECT MESSAGE
(DISPLAY OF GREETING FIELD)
SELECT A MESSAGE (6–8 CHOICES):
HAPPY BIRTHDAY! HAPPY ANNIVERSARY! GREAT JOB!
CONGRATULATIONS! (CUSTOM) (MOTHER'S DAY)
(CHOICES CUSTOMIZED PER KIOSK LOCATION)
BACKUP NO MESSAGE HELP
370
#13A COMFIRMATION OF CUSTOM TEXT
(GRAPHIC OF COMPLETED FIELDS)
GREETING CARD & CERTIFICATE
IS THIS CORRECT?
YES NO
BACKUP HELP
368
#12B
CUSTOM MESSAGE
HAPPY BELATED MOTHER'S DAY,
MOM! REQUIRES ALPHA AND
NUMERIC KEYBOARD
A
372
#13B IF NO
(RETURN TO DISPLAY FIELDS)
WHAT SHOULD CHANGE?
AMOUNT GREETING NAMES STORE
(RETURN TO CATEGORY CHOSEN)
374
IF CREDIT REPORT STILL IN PROGRESS
"CREDIT CARD VERIFICATION IS STILL IN PROGRESS. STAND BY."
(:05 TIME–OUT TO "VERIFICATION IS STILL IN PROGRESS.")

FIG. 10C

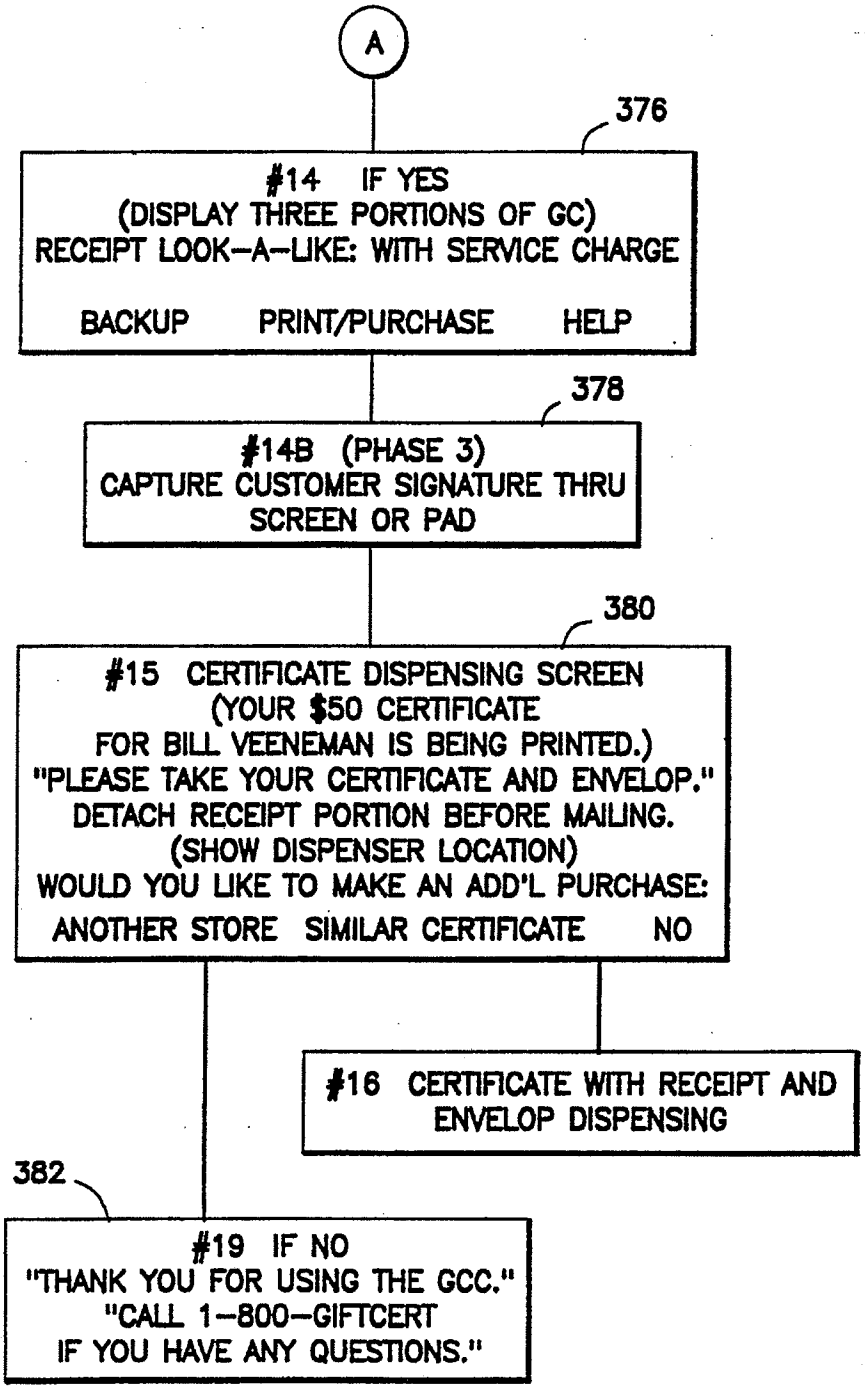


FIG. 10C CONTINUED

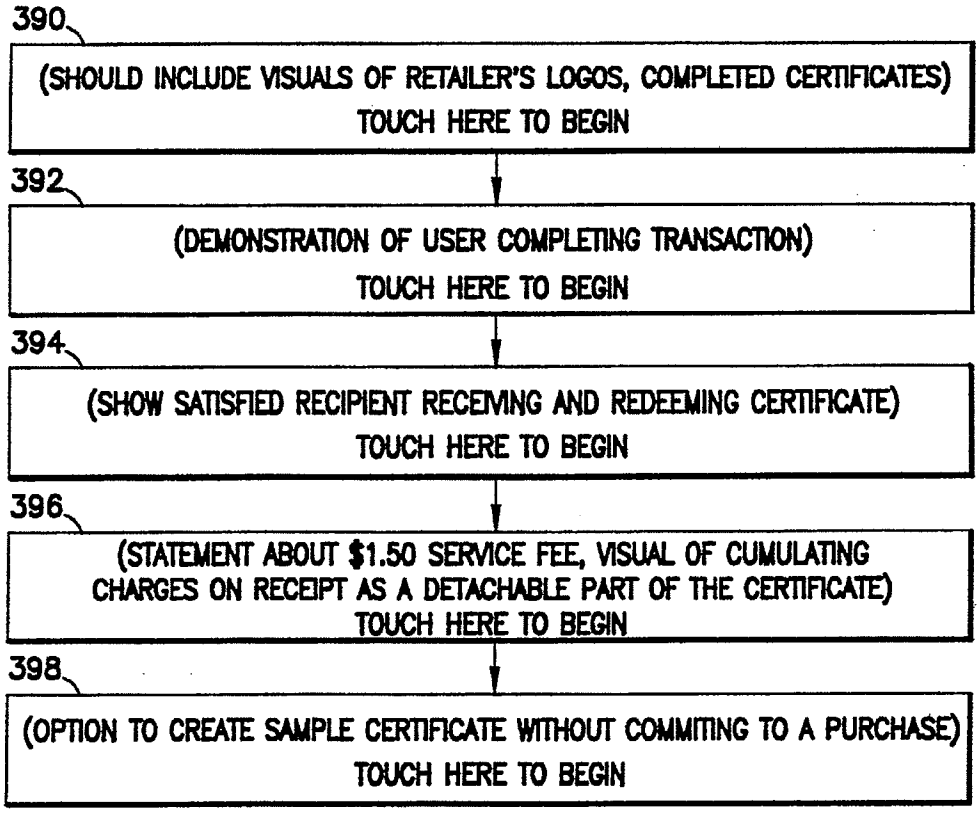

390
(SHOULD INCLUDE VISUALS OF RETAILER'S LOGOS, COMPLETED CERTIFICATES)
TOUCH HERE TO BEGIN
392
(DEMONSTRATION OF USER COMPLETING TRANSACTION)
TOUCH HERE TO BEGIN
394
(SHOW SATISFIED RECIPIENT RECEIVING AND REDEEMING CERTIFICATE)
TOUCH HERE TO BEGIN
396
(STATEMENT ABOUT $1.50 SERVICE FEE, VISUAL OF CUMULATING CHARGES ON RECEIPT AS A DETACHABLE PART OF THE CERTIFICATE)
TOUCH HERE TO BEGIN
398
(OPTION TO CREATE SAMPLE CERTIFICATE WITHOUT COMMITING TO A PURCHASE)
TOUCH HERE TO BEGIN

FIG. 11

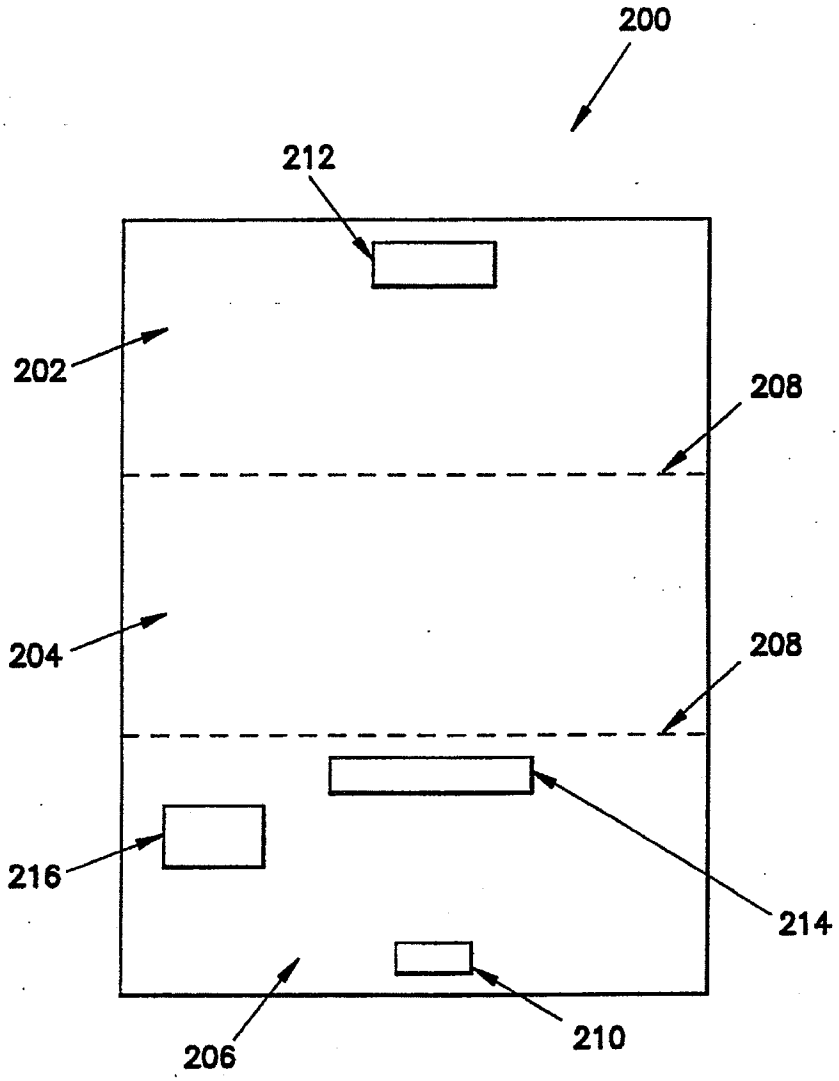


FIG. 12

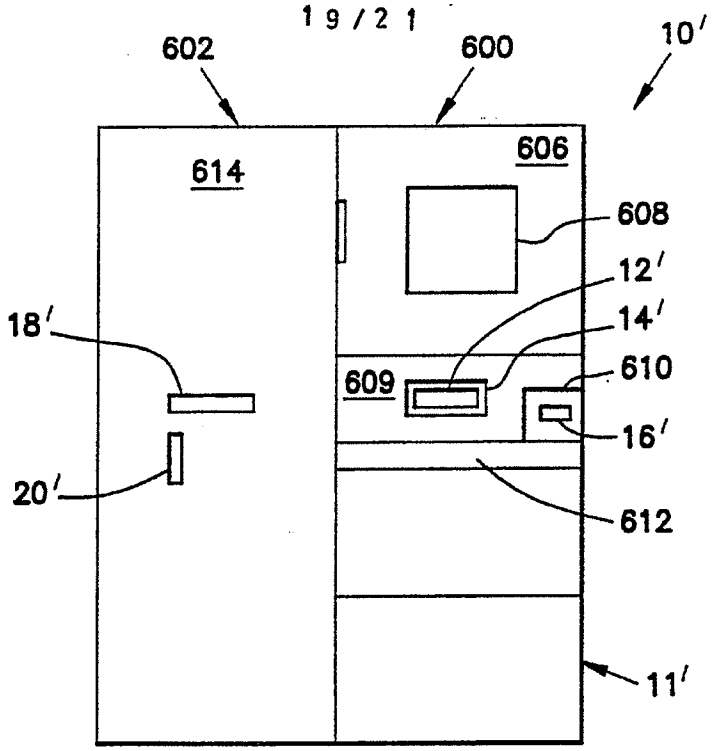

602
600
10'
614
606
608
12'
14'
18'
609
610
16'
20'
612
11'

FIG. 13

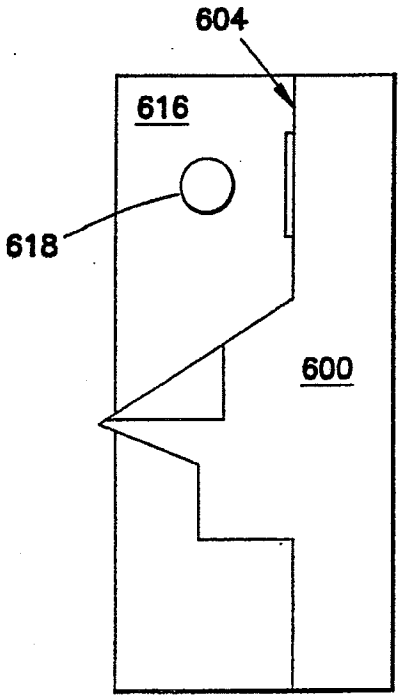

604
616
618
600

FIG. 14

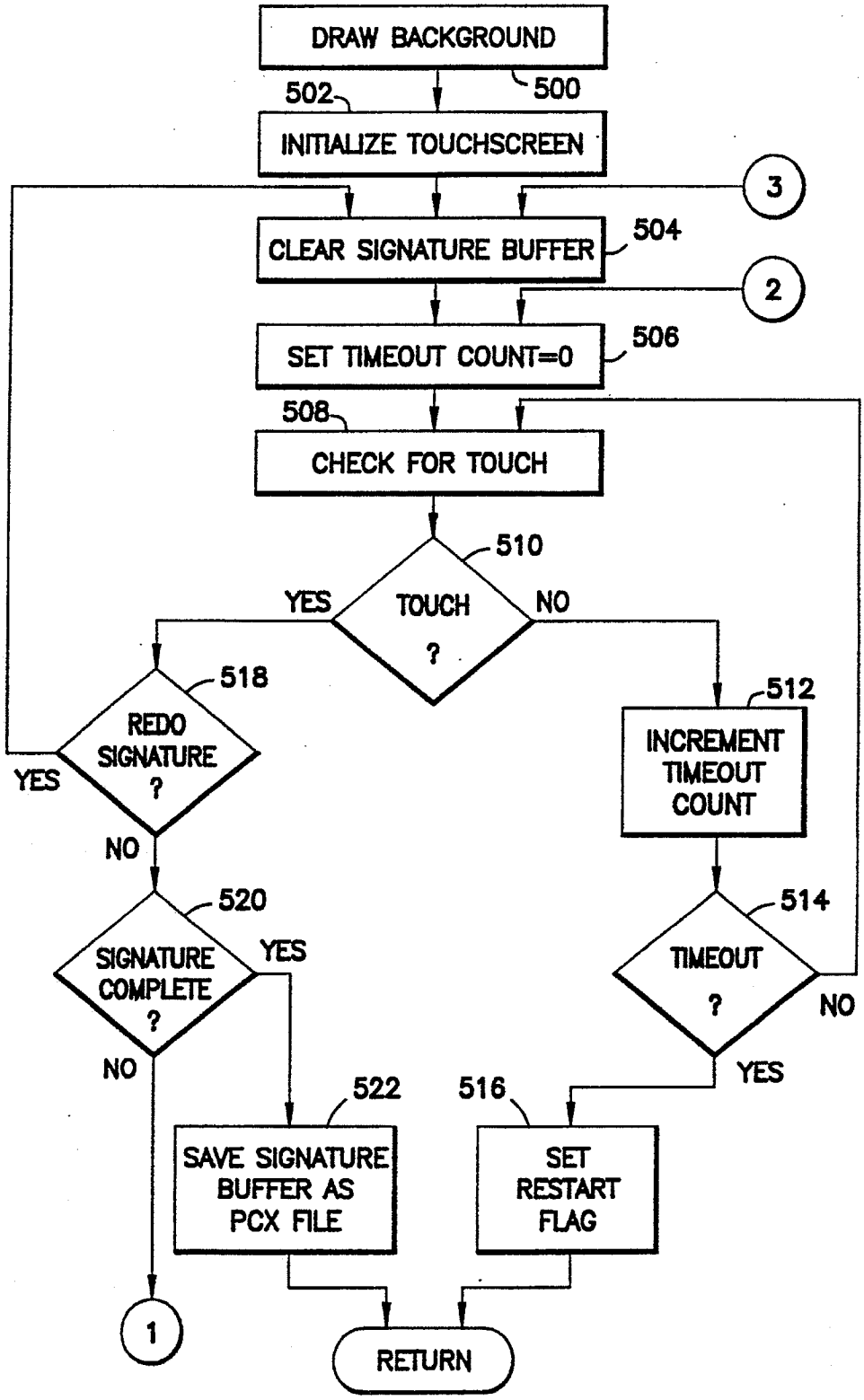

DRAW BACKGROUND
500
502
INITIALIZE TOUCHSCREEN
3
CLEAR SIGNATURE BUFFER
504
2
SET TIMEOUT COUNT=0
506
508
CHECK FOR TOUCH
510
TOUCH ?
YES
NO
518
REDO SIGNATURE ?
YES
NO
512
INCREMENT TIMEOUT COUNT
520
SIGNATURE COMPLETE ?
YES
NO
514
TIMEOUT ?
NO
YES
522
SAVE SIGNATURE BUFFER AS PCX FILE
516
SET RESTART FLAG
1
RETURN

FIG. 15A

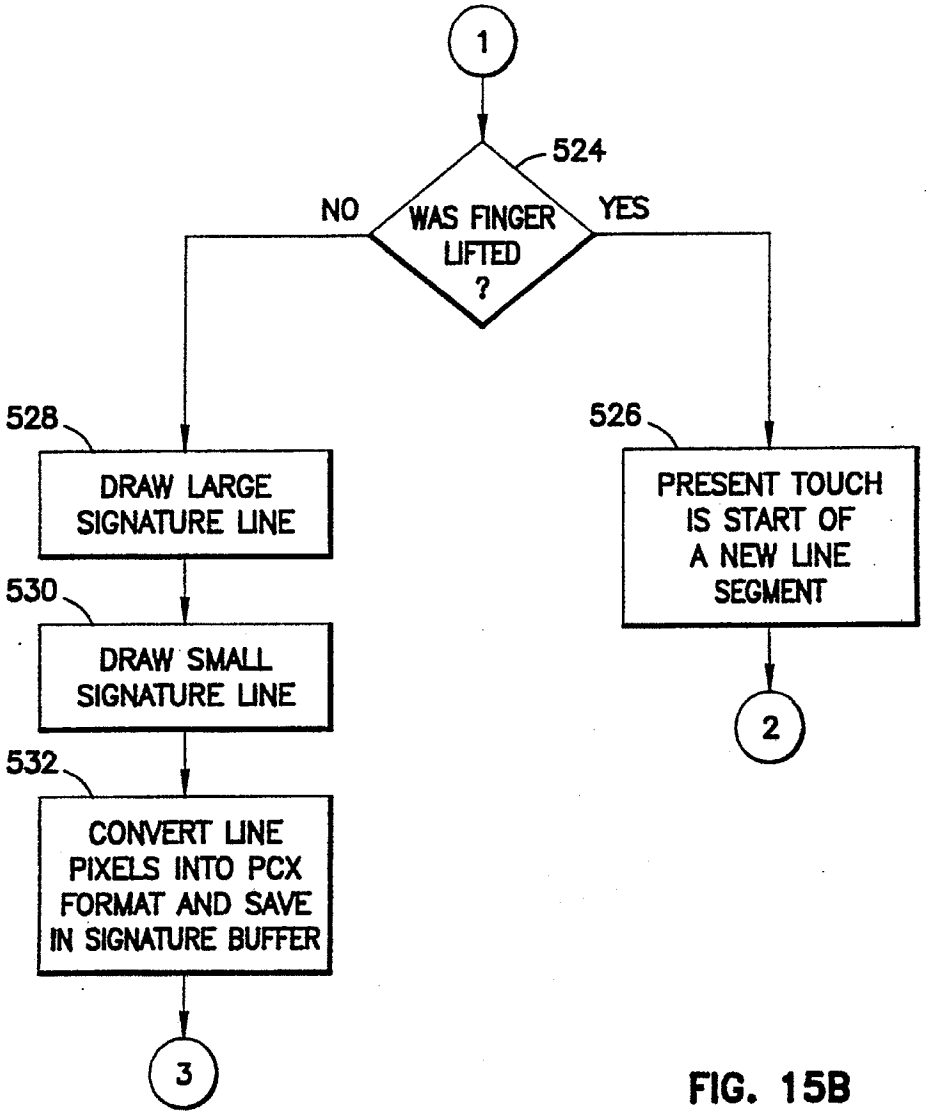

1
524
WAS FINGER LIFTED ?
NO
YES
528
DRAW LARGE SIGNATURE LINE
530
DRAW SMALL SIGNATURE LINE
532
CONVERT LINE PIXELS INTO PCX FORMAT AND SAVE IN SIGNATURE BUFFER
3
526
PRESENT TOUCH IS START OF A NEW LINE SEGMENT
2

FIG. 15B

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 92/01187

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all)[6]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int.Cl. 5 G07B1/02; G07F17/42; G06F15/24

II. FIELDS SEARCHED

Minimum Documentation Searched[7]

Classification System	Classification Symbols
Int.Cl. 5	G07B ; G07F ; G07C ; G06F

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched[8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT[9]

Category °	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No.[13]
Y	US,A,4 359 631 (LOCKWOOD) 16 November 1982 see column 2, line 38 - column 3, line 41 see column 7, line 10 - column 8, line 50; figures	1,2,5,15 22,25
A		3,4, 6-11,24

Y	EP,A,0 114 723 (FUJI XEROX) 1 August 1984 see page 3, line 1 - page 10, line 7; figures	1,2,5,15 22,25
A		8-13,24

A	EP,A,0 119 720 (FUJI XEROX) 26 September 1984 see page 1, line 25 - page 5, line 36; claims; figures	1,8-15 22-25

A	WO,A,8 501 373 (ELECTRONIC ADVERTISING NETWORK) 28 March 1985 see page 6, line 34 - page 16, line 4; claims; figures	1,8-15, 22-25

	-/--	

° Special categories of cited documents :[10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
09 JULY 1992	04. 08. 92
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	MEYL D.

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)

Category °	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.
A	WO,A,8 805 578 (THE SAVINGS SPOT) 28 July 1988 see abstract; claims; figures ---	1,8-15 22-25
A	US,A,4 809 837 (HAYASHI) 7 March 1989 ---	
A	WO,A,8 603 310 (NICHTBERGER) 5 June 1986 ---	

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO. US 9201187 SA 58507

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information. 09/07/92

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US-A-4359631	16-11-82	US-E-	RE32115	15-04-86
EP-A-0114723	01-08-84	JP-A-	59128666	24-07-84
		US-A-	4677551	30-06-87
EP-A-0119720	26-09-84	JP-A-	59146373	22-08-84
		DE-A-	3470620	26-05-88
		US-A-	4604696	05-08-86
WO-A-8501373	28-03-85	US-A-	4674041	16-06-87
		AU-A-	3397984	11-04-85
		EP-A,B	0156856	09-10-85
WO-A-8805578	28-07-88	AU-A-	1496088	10-08-88
		EP-A-	0299061	18-01-89
		JP-T-	1501350	11-05-89
		US-A-	4896791	30-01-90
US-A-4809837	07-03-89	JP-A-	60220485	05-11-85
WO-A-8603310	05-06-86	US-A-	4882675	21-11-89
		AU-A-	5094485	18-06-86
		CA-A-	1276724	20-11-90
		EP-A-	0203958	10-12-86

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/02, 9/08

A1

(11) International Publication Number: **WO 95/26014**

(43) International Publication Date: 28 September 1995 (28.09.95)

(21) International Application Number: PCT/GB95/00596

(22) International Filing Date: 17 March 1995 (17.03.95)

(30) Priority Data:
9405362.6 18 March 1994 (18.03.94) GB

(71) Applicant *(for all designated States except US)*: TRANSMO LIMITED [GB/GB]; Moat House Business Centre, Melbourn Science Park, Melbourn, Royston, Hertfordshire SG8 6EJ (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: STANFORD, Christopher, John [GB/GB]; 19 Roundwood Lane, Harpenden, Hertfordshire AL5 3BW (GB). DE JONG, Eduard, Karel [NL/NL]; Maliebaan 4, NL-1097 HS Amsterdam (NL).

(74) Agent: NASH, Keith, Wilfred; Keith W. Nash & Co., Pearl Assurance House, 90-92 Regent Street, Cambridge CB2 1DP (GB).

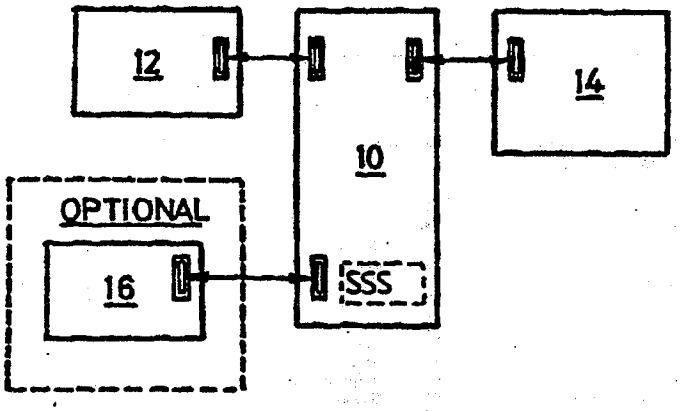
(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TT, UA, UG, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: IMPROVED CARD CHARGING SYSTEMS

(57) Abstract

A security device for use in a card charging system where a service or product providing facility issues services or products by the use of credit from a card. The security device comprises signal transmission means for delivering signals to a purchasing facility to enable a user to acquire a service or product dependent on the credit debited from a card, a record keeping subsystem to certify the credit debited from the card and to identify which account is to receive the debited credit and signal processing and output means for generating signals indicating a successful transaction. The signals may be encoded by use of encryption techniques. A separable security subsystem provided to ensure a record of transactions is available if power fails on the main security device.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SI	Slovenia
SK	Slovakia
SN	Senegal
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

Title: Improved card charging systems

Field of invention

This invention concerns card charging systems of the type in which a pre-programmed card is read and validated by a suitable card reader and data stored on the card is decremented according to the cost of a purchase and made available to the user after the transaction. The invention is concerned with a security device to be installed in such a system to ensure correct control between the card read/write unit and a transaction recording - payment collection system so as to form an integral part of the revenue allocation process.

Background to the invention

It is known to provide coin, token or card operated mechanisms for the collection of payment for goods or services such as bus fare collection systems, pay and display parking devices, prepared food delivery systems and the like. Such devices may be capable of debiting prepaid or credit cards such as the systems currently in use for the provision of telecommunication services and the concept of a prepayment credit card for obtaining bus journeys and tickets for train journeys has already been tried.

It is an object of the present invention to enable such systems to accept a universal prepurchased stored value or debit card and to allow the amount which has been debited from the card to be allocated to the appropriate service or goods provider.

Summary of the invention

According to the present invention there is provided a security and transaction device for use in connection with a card

read/write device, comprising; signal transmission means for delivering signals to a host facility to enable a purchase to be made in return for an amount of credit debited from a card after the latter has been read by a card reader, which signals comprise a unique identification number together with signals defining a public key-based security system; a record keeping subsystem adapted to certify a credit debited from the card and identify which one of a plurality of accounts is to receive the debited credit; and signal processing and output means for generating signals indicative of a successful transaction and of an appropriate form and value so that in use the generated signal indicates to the host facility the nature of the transaction completed and the purchase which is now to be made available.

The host facility may be a service providing facility where the purchase involves provision of a service such as transportation, seating in an auditorium or the like.

Alternatively the host facility may be a product providing facility where the purchase involves supply of a product such as foodstuffs, clothing, medication and the like.

Optionally the device includes a smart card reader and further signal processing means, whereby a smart card open payment system may be employed in lieu of a prepayment credit card system, for payment for a service or commodity.

According to one embodiment of the invention a security module is provided in connection with each transaction recording system which is adapted to receive a specific machine readable card and the security module serves to ensure correct control between the card read/write unit and the host controlling equipment to which it is attached.

Thus in the case of a bus fare collection system, pay and display parking and the like, the security module is situated

between the card reader and the mechanism for dispensing a bus ticket or pay and display parking ticket or the like.

In this embodiment the security module forms an integral part of the revenue allocation process since the security module enables the issuer of the card to be identified and thereby enables the service or commodity provider to identify the organisation from which it is to recover the funds relevant to the transaction provided by the service or commodity provider.

It is a characteristic of the system proposed by the invention that no direct link between service provider and issuer need exist if a centralised accounting facility is provided with credit and debit accounts for each of the issuers and/or service or commodity providers. (It is to be understood that both issuers and service/commodity providers may be one and the same, but in the general case they need not be). By matching transactions identified as credits to a service or a commodity providers account against a corresponding debit for the same amount as the transaction in an issuers account, so the overall debit/credit position remains neutral.

Even if the card has been purchased from the organisation providing the service, the principle holds good since the service provider (or commodity provider) who has sold the card in the first place will have had an overall debit equal to the value of the card entered on its debit account and when the card is used to purchase its services or commodities, the corresponding credits would appear in its credit account neutralising the transaction. The money received for the card will remain in the service or commodity providers hands and if the total value of the card is used to purchase services or commodities provided by the same organisation who issued the card, the net effect is simply that the person purchasing the card has paid in advance to the same organisation the necessary funds to obtain the subsequent services or commodities or both from that self same organisation.

Where the card is purchased from an issuer then the issuers account is debited by the total value of the card and is subsequently credited as the card is used to purchase services or commodities from other organisations. At the end of any accounting period the debit and credit position of the various organisations whether issuing cards or providing services or commodities or both, is balanced off and any net inflow of funds necessary to balance the accounts is requested by the central billing organisation of the different organisations as appropriate.

Typically the machine readable card is a magnetic strip card capable of being read and written to by appropriate card read/write devices.

According to a particular preferred feature of the invention, the security module is adapted to recognise a specific identification code and card issuer identification details from a datastream derived from the card and passing between the card reader and host equipment. The security module deduces the value of the successful transaction and adds this to the total value collected for each card issuer and is stored within the security module.

Preferably the total value collected and the identification information and the like is digitally certified.

Preferably the data is stored in a non-volatile manner in a memory associated with the security module.

Preferably the memory is a non-volatile memory and is located in a security subsystem.

Preferably the subsystem is separable from the remainder of the security module or from a part thereof to enable it to be removed, for example from a vehicle such as a bus for park and display ticket issuing, and data therein downloaded into a host

computer for processing and updating the accounts of card issuers and host facilities, such as service/commodity providers as aforesaid.

In order to build in an audit trail, a new total value for each issuer and previous totals of all cards from all issuers that have been accepted by a particular service host (eg ticket issuing device) are certified with a digital signature and transmitted to the service host at the end of each transaction. Thus the security module not only retains within its security subsystem a complete record of accumulated totals for each card issuer, but this information is also stored in the service host such as a ticket issuing machine memory. In the event of lost records, details of the transactions associated with the service host can be retrieved from the security subsystem of the security module and vice versa.

According to a preferred feature of the invention, although the security subsystem is primarily concerned with payment records, additional information may be read and written to the cards by some service providers and to facilitate this the security module must provide a data highway between the host equipment and the card read/write unit to enable the service host such as a ticket issuing machine to transfer the data to the card. To this end the security module of the invention needs to appear transparent between the card read/write unit and the service host at least as regards such additional information.

In one particular system, involving the issue of tickets on a bus, at the end of a shift or service providers accounting period, all of the individual issuer totals accumulated in the service host memory are collected from the service host by whatever method the service provider chooses. Typically transportable modules are employed in the case of buses, on-line or via portable data collection terminals in the case of pay and display equipment or even paper records as appropriate. It is to be noted that although reference is made

here only to service provider, the term is intended to include commodity providers.

The information relating to individual issuer totals is preferably fed into data concentrating host computers held by the service providers for later polling by an accounts clearing centre.

Since the security module subsystem memory stores separate and duplicated non-resettable totals for every issuer whose cards have been used in the particular service host in which the security module is installed, in the event of records being lost, the next time that records are collected from the service host they will be recovered.

In the event of a complete equipment breakdown, the security module can be removed from the equipment and either of the duplicated records stores accessed by the clearing centre to recover the data.

Preferably each security module holds a unique identifier which is used to identify the service host to which it is fitted and with which it has been used.

Preferably the security subsystem is a tamper resistant single integrated circuit device or chip which has a built-in processor and co-processor capable of generating irrefutable digital signatures at high speed. Preferably it also has sufficient non-volatile storage to hold totals for a large number of issuers typically 500 issuers. This security system can be externally powered separately from the rest of the security module circuitry such that contents can be accessed by the central accounts facility even if the majority of other components within the security module are down or have become faulty.

The digital signatures are generated using public key

cryptographic methods. This means the clearing centre and any issuer can verify the correctness of the signed files but cannot themselves generate the signatures, ie create new files.

If any records are tampered with along the route from service providers equipment to the clearing centre, it will be discovered. Likewise, preferably means is embedded in the security architecture to detect duplicated records and to detect if records are missing.

As previously indicated, preferably after each transaction the new total is signed with a digital signature and the digital signature generation is likewise preferably based on a public key system (RSA or equivalent) and the security module provides a tamper resistant storage of secret keys.

Preferably the security module is capable of generating the digital signature aforesaid in less than one second.

The result of each transaction together with the signature is stored in the security subsystem as aforesaid and is also transmitted to the surface host equipment for storage therein.

Preferably when a security module is removed from its normal installation (for example for reconciliation where all other means cannot be used), then the card reader should be disabled and the ability to generate valid certificates is lost until the or another security module is inserted.

Preferably the collection of data pertaining to the payment transactions as registered by the combined security module and security subsystem module is handled in accordance with a formally defined protocol. In a preferred arrangement the protocol is based on maintaining a running total of transaction values.

The main part of the protocol is implemented in the security

subsystem. To this end it may secure in permanent (non-volatile) memory of the security subsystem device, two running total counters (a running total of transaction values and a running total of the number of transactions), are kept for each issuer of cards. After each transaction the security subsystem is adapted to compute a digital signature on the latest value of the stored counters and the digital signature warrants the validity of the counter values as it is based on the unique secret encryption key stored in the security subsystem.

The digital signature enables the validity of the counter values to be warranted since it is based on a unique secret encryption key stored in the security subsystem.

Preferably after obtaining the digital signature the security module continues the protocol and together with accumulating countervalues which the security module maintains in parallel in its own memory, the new signature is packed into a number of records and transferred to the service host.

A final step of the protocol is performed in the central clearing facility which is adapted to receive the records from a security module through its connection with an acquirer host. The clearing centre retrieves from its storage the last known values of the accumulating countervalues from this host. In subtracting the corresponding counters in the received and the stored records, the net amount spent with cards for each issuer can be computed and the computed amount logged on disc and paper as appropriate.

The transfer of money based on the computed results does not form part of the protocol but can be effected as soon as the computed amounts have been determined and stored.

It will be seen that the protocol as outlined is immune to any disruption, accidental or purposeful of the communication from

the security module to the central clearing centre. In particular, the connection between service host and acquiring host is assumed to be unreliable where records may get lost or be duplicated without consequence. Primarily the protocol is protected by the digital signature and subsidiary protection is obtained by inclusion of the security subsystem and security module identity numbers and account of the current number of transactions in the signed message.

As increased numbers of issuers are recognised by the system, the number of totals kept within each security module will increase. Whilst the security module can handle sufficient issuer totals the transmission on every occasion of the records relating to for example 500 issuers becomes time consuming and could effect the ability of a particular service host to process transactions at high speed.

According therefore to a preferred feature of the invention, means is provided within the security module to determine whether or not to include the total from each of the records and a criterion for determining not to include the total from a particular record may be linked to time during which there has been a lack of activity in relation to that particular total.

Typically the time interval is determined by the total number of transactions carried out by the security module since the last change made to any particular total. The value of this number (of transactions) is set by the maximum number of transactions per day plus a significant safety margin to ensure that several copies of the records containing the final value of the total about to be omitted have been captured by the clearing centre. This may be determined by examination of the transaction history files accumulated at the transaction clearing centre.

According to a further preferred feature of the invention, each

security module includes means for storing and generating a secret key which is used to generate a digital signature based on a public key scheme (RSA or equivalent) and periodically the secret key used by the security module is changed.

The change may be automatic in a pseudo-random manner as determined by for example the overall number of transactions processed by the security module.

Preferably the key change instances are known to the clearing centre for each security module on an individual basis so that this information can be logged and used in decoding and auditing reports from security module data.

The invention will now be described in outline only by way of example with reference to the accompanying drawings in which:

Figure 1 shows a security module inserted into an existing card accepting payment system;

Figure 2 shows the essential parts of a security module in accordance with the invention; and

Figure 3 which is a block diagram illustrating the overall charge and accounting system utilising the security module provided by the invention for identifying the card issuers who are to be credited with transactions as they occur.

Detailed description of drawings

Figure 1 shows the security module 10 of the invention located between a magnetic card read/write device 12 and a conventional service or commodity providers apparatus for supplying a service or a commodity as appropriate such as a card operated ticket dispenser 14.

The Magnetic card read/write device 12 may be, for example, one

as supplied by GPS Card Technology. Suitable card operated ticket dispenses are Wayfarer's 3 and Metric Autoslot.

In known manner the latter is designed to be operated by means of prepayment cards of a particular type and the module 10 of the invention allows cards other than those purchased from the service/commodity provider to be used to purchase the service or commodity concerned.

An optional extra comprises a smart card read/write device 16 by which a so-called smart card can be used to purchase the service or commodity in lieu. Typical smart card read/write devices are supplied by Schlumberger.

Figure 2 shows the essential parts of the security module 10.

A data path 18 from the magnetic card reader 12 and the data path 20 from the smart card reader 16, supply data as appropriate to two data inputs of a multiplexer (MUX) 22. Data from MUX 22 is supplied over a data path 24 to the host equipment such as the card operated ticket dispenser previously referred to. Such devices have been used on buses and as car park ticket dispensing machines.

The module 10 includes a unique identification number stored within a memory 26 in the device which is used in conjunction with a public key based security subsystem which performs a certification of values collected from cards inserted into the reader 12.

A programmable controller 28, for example a Zilog Z80, receives data from the MAX 22 and after processing, transmits data to the MUX along data path 30.

The memory 26 additionally stores data.

A security subsystem 32, for example an ATMEL AT8SC54C, which

includes a second processor, serves to archive records (files) of all successful transactions. To this end the security module processor 28 deduces the value of each successful transaction from the data supplied to or from the card and adds this value to the total value collected for each card issuer (who may also be another service/commodity supplier), and to this end each card includes an issuer identification code which is transmitted in the datastream passing between the card reader 12 and the host equipment 14. Typically a look-up table of issuers and identification codes is contained in the computer store 26.

A running total of each issuer is retained in a nonvolatile archive memory in 32 and the appropriate total is updated at the end of a transaction. The data is certified as previously described by means of a digital signature corresponding to the issuer (identified from the data read from the card via MAX 22) and the same information is transmitted along with the new total value for the issuer concerned to the host equipment, for storage in the memory therein in manner known per se.

In this way the transaction value data and card issuer data is archived in the two separate locations and this double redundancy ensures that a full audit trail will always remain to allow the recovery of lost records in the event that one or the other of the archived data is lost.

Power for the security module is typically obtained from the host power supply, usually a DC supply. The power supply for this device 10 is denoted by reference numeral 34. Connections to the host equipment are not shown but the unit may be adapted simply to be plugged into a multiway socket or the like.

In accordance with the method of the invention at the end of a given period (such as a shift for a bus crew or a day or week for a car parking ticket dispensing facility), the data archived in 32 is accessed and read out and transferred to a

computer memory in any convenient manner. Thus modules removable from the equipment mounted in a bus may be removed and the data downloaded to a computer at a remote position or on-line or portable data collection devices may be used to transfer data from 32 without the need to remove any unit from the equipment. If a printer is employed, the data may instead or in addition be made available as paper records.

Data concentrating and collecting computers operated by the service/commodity provider(s) (not shown) serve to hold the totals for the different card issuers and this data is available to be downloaded to a central data processing centre (not shown) to enable recharging of the card to purchase service/commodity to be performed.

Since the security module 10 includes a non-volatile memory 32 in which non-resettable totals of transactions values for each issuer whose cards have been used to purchase the particular service or commodity, controlled by the host equipment to which it is connected, in the event of records being lost, then the next time records are collected from the service/commodity host equipment, the records which have been lost will be recovered.

If there is a complete equipment breakdown the security module can be removed from the host and either of the duplicated record stores accessed to remove the data.

As a further security means, the security module 10 holds a unique identifier by which the service host to which it is fitted can be identified.

Security subsystem (SSS)

Item 32

Typically this is a tamper resistant single smart card chip which has a built in processor and co-processor capable of

generating irrefutable digital signals quickly. It also has sufficient non-volatile storage to hold totals from a large number of issuers. Typically the capacity is 500 issuers. This security system can be externally powered separately from the rest of the security module (SM) 10 circuitry such that its contents can be accessed to a central controller even if other components within the SM are faulty.

The digital signatures are generated using public key cryptographic methods. This means a central controller such as is associated with a clearing centre, and any issuer can verify the correctness of the signed files but cannot themselves generate the signatures (ie create new files). If any records are tampered with along the route from a service commodity providers equipment to the clearing centre, it will be discovered and likewise embedded in a security architecture is the means to detect duplicated records and whether or not records are missing. After every transaction the new total is signed with a digital signature.

The digital signature generation is based on a public key scheme (RSA or equivalent) and the SM 10 provides tamper resistant storage of secret keys and is capable of generating a digital signature in less than one second. The result is stored in the security subsystem 32 and sent to the service host.

If the SM is removed (for a reconciliation when all other means cannot be used), the card reader must be disabled and of course the ability to generate valid certificates is lost until another SM is inserted.

The data accumulation protocol

The collection of data pertaining to payment transactions as registered by the SM 10 - SSS 32 combination, is handled following a formally defined protocol. This is based on

maintaining a running total of transaction values.

The main part of the protocol is implemented in the SSS 32. In the secure and permanent non-volatile memory of this device two accumulation counters (running totals of transaction values and number of transactions) are kept for each issuer of cards. In principle after each transaction the SSS 32 computes a digital signature on the latest value of the stored counters. The digital signature warrants the validity of the counted values as it is based on a unique secret encryption key stored in SSS 32.

After obtaining the digital signature the SM 10 continues the protocol. Together with accumulation countervalues which the SM maintains in parallel in its own memory, the new signature is packed into a number of records and transferred to the service host.

In a later protocol step, the clearing centre (CC) (not shown) receives the records from an SM 10 through its connection to an acquirer host. The CC retrieves from its storage the last known values of the accumulation counters from this host. By subtracting the corresponding counters in the received and stored records, the net amount spent using cards from each issuer is computed. The computed amount is logged on disc and/or paper.

The monetary value based on the computed results is transferred between the issuers records to adjust the issuers balances to show what is owed to who.

The accumulation counter protocol is immune to disruption whether accidental or intentional of the communication from SM to CC. In particular the connection between service host and acquiring host is assumed to be unreliable and that records may get lost or be duplicated without consequence. Primarily the protocol is protected by the digital signature subsidiary

protection being obtained by inclusion of SSS and SM identity board numbers and account of the current number of transaction in the signed message.

Ageing

As more and more issuers are recognised by a system the number of totals kept within each SM 10 increases. Whilst each SM can handle a large number of issuer totals, the transmission of records relating to up to 500 issuers becomes time consuming and could affect the ability of a particular service host to process transactions at full speed. To this end the SM is provided with decision making circuitry to omit totals from the records after a suitable interval of inactivity. This interval is determined by the total number of transactions carried out by the SM since the total about to be omitted was last changed. This last number is set by the maximum number of transactions per day plus a significant safety margin to ensure that several copies of records containing the final value of the total amount to be omitted have been captured by the clearing centre. The parameters on which to base decisions to omit can be determined by examination of the transaction history files accumulated at the clearing centre.

Key changes

Periodically the secret key used by the SM 10 to generate the signature may be changed. In one preferred arrangement this is effected automatically in a pseudo-random manner as determined by the overall number of transactions processed by the SM. These key change instances will be known to the clearing centre for each SM on an individual basis.

Figure 3 shows in a simplified manner how data relating to different card issuers accounts can be updated periodically for example at the end of each shift in a bus company operation or

at the end of each day or week in the case of car parking facilities. The system shown in Figure 3 does not include the signature generation and data verification steps but is intended merely to show how cards may be sold freely and provided the cards contain the appropriate identification data, can be used to purchase services or commodities from either the original issuer or another organisation or service or commodity provider and how the latter can obtain the necessary credit from a central clearing facility in return for providing the service or commodity required.

In order to simplify matters, only four card issuers are shown and each of the card issuers is also assumed to be a service or commodity provider. To this end card issuing and card operated facilities belonging to each of the four organisations are denoted by the same letter. Again for simplification only one card issuing facility is shown for each of the organisations and one card operated service or commodity provider for each organisation. In practice there may be many card issuing facilities associated with each organisation and many different service and/or commodity prcviding card operated facilities also owned and operated by the same organisation. Likewise the system is not limited to four issuers/providers but any number can be accommodated, the only limit being the size of the memory capacity of the computers involved. As will be seen later, a card issuer need not also be a commodity or service supplier but may simply be a card issuing facility. In addition a commodity or service provider need not themselves be a card issuing organisation although in general it is expected that they will wish to do so.

A card is issued by the insertion of money (denoted by a £ sign) and the money is retained by the issuer as shown at 38 and this enables further supplies of cards 40 to be purchased for future sale.

The card may be used to purchase any one of four issuers

services or commodities. By way of example a card issued by organisation A is shown being used to purchase a commodity valued at £N from a commodity supplier D. To this end the card (identified by 42) and identifiable as being one issued by issuer A, is inserted into a card reader 44 associated with a security module 46 such as 10 in Figure 1 and a commodity dispenser 48 (such as 14 in Figure 1). Data corresponding to £N is coupled with the unique identification linked to supplier A and is stored in 46 and 48 as already described.

At the end of the accounting period this data is transferred to a host computer 50. The latter is polled or otherwise accessed at intervals and the transaction data stored therein is downloaded along data paths 52 and 54. The first is a debit highway and the £N value of the transaction so far described is debited from an account stored in an up/down memory 56 for issuer A and the same value of £N is credited via a credit highway 54 to the account stored in another up/down counter 58 for the commodity supplier D.

Debiting and crediting is achieved by means of addressing circuits 60 and 62.

In order to provide a full audit trail the unique transaction data linked to each transaction by the security module is stored as part of each value in each memory 56, 58 etc.

The current total for each issuer can be obtained by addressing means 64 which causes related to the selected memory to be delivered along highway 66 to a printer 68 to deliver printed statements-to the users. In addition or alternatively the data on 66 may be used to automatically debit or credit a bank account designated by the issuer/user concerned.

In the same way a card purchased from issuer C may be used to acquire a commodity from B in which event the value of the transaction will be debited from memory 70 and credited to

memory 72.

When cards to a value of £X are purchased by an issuer, the issuers memory 56, 58, 70 or 72 as the case may be is credited with the corresponding value of £X.

It should be noted that an issuer does not need to be a service or commodity supplier. Thus if C is merely a card selling facility but A, B and D are suppliers of services and/or commodities, the memory 70 will only ever be credited whenever cards are purchased for resale by C but will always be debited whenever one of its cards is used to purchase a service or commodity from A or B or D. No card transaction will ever credit memory 70.

On the other hand if B not only provides a service (for example) but also purchases cards for resale, and serves as a card issuer as well, memory 72 will be credited whenever B purchases cards for resale and whenever a card is used to purchase B's service and will be debited whenever a card sold by B is used to purchase another supplier service or commodity.

The crediting of the memories A, B, C, D is achieved by a process 74 and data highway 76. Only four issuers A, B, C and D are shown in Figure 3 but it is to be understood that any number can be accommodated, it being necessary merely to increase the number of memories 56, 58 etc and the addressing capabilities of the buffer 60 and 62.

Additionally, although only card issuing facility associated with supplier A is shown at A' and one service providing facility belonging to supplier A at A'', any number of issuing stations may be provided such as A', and any number of service providing facilities (such as A''), for the supplier A. The same applies to all of the other users of the system.

The data highways 52, 54 and 76 may be permanent land lines,

radio, infra-red or optical links, or may simply illustrate the direction in which data is to be transported as by disc or tape or in a solid state memory device from one location to another.

Claims

1. A security and transaction recording device for use in connection with a card read/write device comprising; signal transmission means for delivering signals to a host facility to enable a purchase to be made in return for an amount of credit debited from a card after the latter has been read by a card reader, which signals comprise a unique identification number together with signals defining a public key based security system; a record keeping subsystem adapted to certify a credit debited from the card and identify which one of a plurality of accounts is to receive the debited credit; and signal processing and output means for generating signals indicative of a successful transaction; so that in use the generated signals indicate to the host facility the nature of the transaction completed and the purchase which is now to be made available.

2. A security device according to claim 1, wherein the host facility is a service providing facility for supply of a service.

3. A security device according to claim 1, wherein the host facility is a product providing facility for supply of a product.

4. A security device according to any of claims 1 to 3, wherein the machine readable card is a magnetic strip card capable of being read and written to by appropriate card read/write devices.

5. A security device according to claims 1 or 2 or 3, wherein the card is a smart card and the device includes a smart card reader and further signal processing means, whereby a smart card open payment system is employed in lieu of a prepayment credit card system.

6. A security device according to any one of claims 1 to 5, wherein a security module is provided in connection with each transaction recording system which is adapted to receive a specific machine readable card and the security module serves to ensure correct control between the card read/write unit and the host controlling equipment to which it is attached.

7. A security device according to claim 6, wherein the security module is adapted to recognise a specific identification code and card issuer identification details from a datastream derived from the card and passing between the card reader and host equipment.

8. A security device according to claim 7, wherein the security module deduces the value of a successful transaction and adds this to the total value collected for each card issuer, the total value being stored within the security module.

9. A security device according to any of claims 1 to 8, wherein the data values associated with the security device are digitally certified.

10. A security device according to any of claims 6 to 9, wherein the data is stored in a non-volatile manner in a memory associated with the security module.

11. A security device according to claim 10, wherein the memory is a non-volatile memory and is located in a security subsystem.

12. A security device according to claim 11, wherein the security subsystem is separable from the remainder of the security module to enable it to be removed and data therein downloaded into a host computer for processing and updating the accounts of card issuers and host facilities.

13. A security device according to claims 11 or 12, wherein the security subsystem is a tamper resistant single integrated circuit device which has a built-in processor and co-processor capable of generating irrefutable digital signatures at high speed.

14. A security device according to claims 11, 12 or 13, wherein the security subsystem has sufficient non-volatile storage to hold totals for a pluraity of issuers.

15. A security device according to claims 11, 12, 13 or 14, wherein the security subsystem is externally powered separately from the rest of the security module circuitry such that its contents can be accessed by a central clearing facility connected to a host facility.

16. A security device according to any of claims 10 to 15, wherein the collection of data pertaining to the payment transactions as registered by the combined security module and security subsystem is handled in accordance with a formally defined protocol.

17. A security device according to claim 16, wherein the main part of the protocol is implemented in the security subsystem, such that the security subsystem is adapted to compute a digital signature on the latest value of the transaction data and the digital signature warrants the validity of the transaction data.

18. A security device according to claim 17, wherein the security module continues the protocol after obtaining the digital signature and together with accumulating counter values which the security module maintains in parallel in its own memory, the new signature is packed into a number of records and transferred to the host.

19. A security device according to claim 18, wherein the

central clearing facility is adapted to receive the records from a security module through its connection with an acquirer host, so that in use the clearing facility retrieves from its storage the last known values of the accumulating countervalues from the host and computes and stores the net amount spent with cards for each issuer.

20. A security device according to any of the preceding claims, wherein a new total value for each issuer and previous totals of all cards from all issuers that have been accepted by a particular service host are certified with a digital signature and transmitted to a service host at the end of each transaction so as to build an audit trail.

21. A security device according to any of the preceding claims, wherein a data highway is provided between the host equipment and the card read/write unit to enable the host to transfer the data to the card, so that in use additional information may be read and written to the cards by host providers.

22. A security device according to any of the preceding claims, wherein each security module holds a unique identifier which is used to identify the service host to which is it fitted and with which is has been used.

23. A security device according to any of the preceding claims, wherein a digital signature for each signal is generated using public key cryptographic methods so as to allow verification of the correctness of the signed signals.

24. A security device according to any of the preceding claims, wherein means is embedded in the security architecture to detect duplicated records and to detect if records are missing.

25. A security device according to any of claims 6 to 24,

wherein each new total is signed with a digital signature based on a public key system and the security module provides a tamper resistant storage of secret keys.

26. A security device according to claim 25, wherein the security module is capable of generating the digital signature in less than one second.

27. A security device according to any of claims 6 to 26 wherein the card reader is disabled on removal of the security module, so that the ability to generate valid certificates is lost until the or another security module is inserted.

28. A security device according to any of the claims 6 to 27, wherein means is provided within the security module to determine whether or not to include the total from each of the issuer records.

29. A security device according to claim 28, wherein a criterion for determining not to include the total from a particular issuer record is linked to a time interval during which there has been a lack of activity in relation to that particular issuer record total.

30. A security device according to any of claims 6 to 29, wherein the security module includes means for storing and generating a secret key which is used to generate a digital signature based on a public key scheme and periodically the secret key used by the security module is changed.

31. A security device according to claim 30, wherein the change in the key is automatic is a pseudo-random manner as determined by the overall number of transactions processed by the security module.

32. A security device according to claims 30 or 31, wherein the key change instances are known to the clearing facility so

that this information can be logged and used in decoding and auditing reports from security module data.

33. A security device substantially as herein described with reference to and as illustrated in the accompanying drawings.

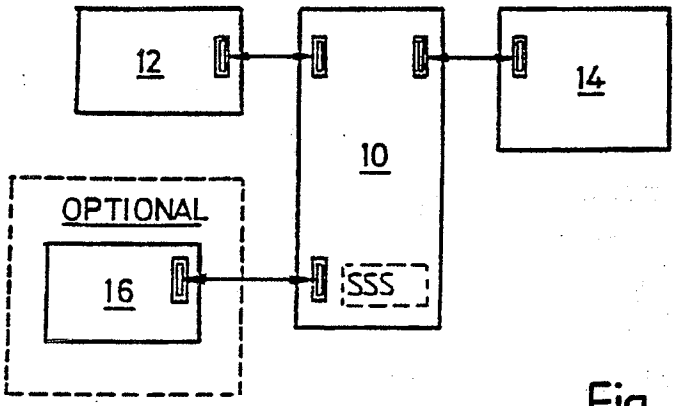

12
14
10
OPTIONAL
16
SSS

Fig. 1

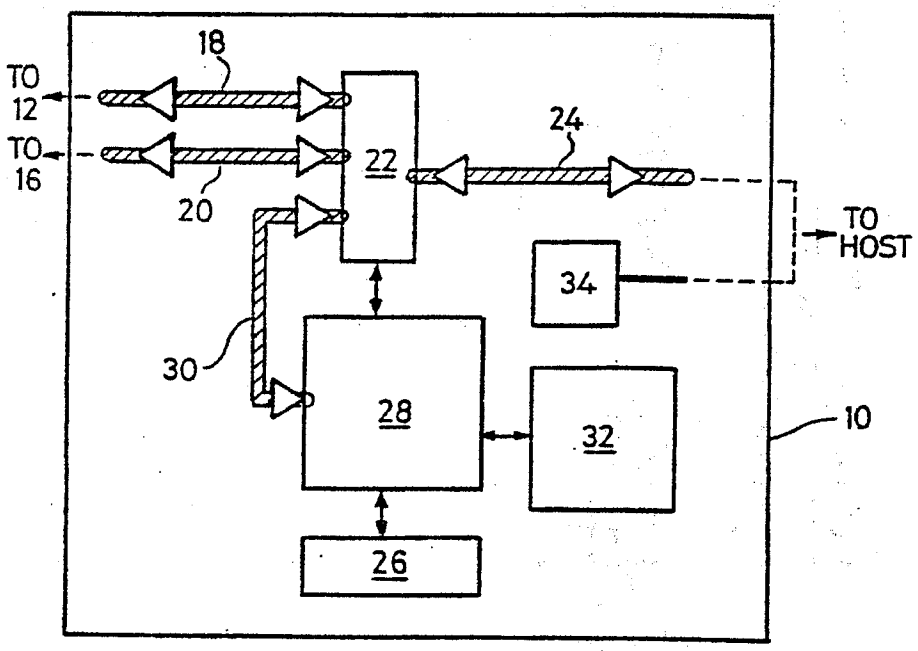

18
TO 12
TO 16
20
22
24
TO HOST
34
30
28
32
10
26

Fig. 2

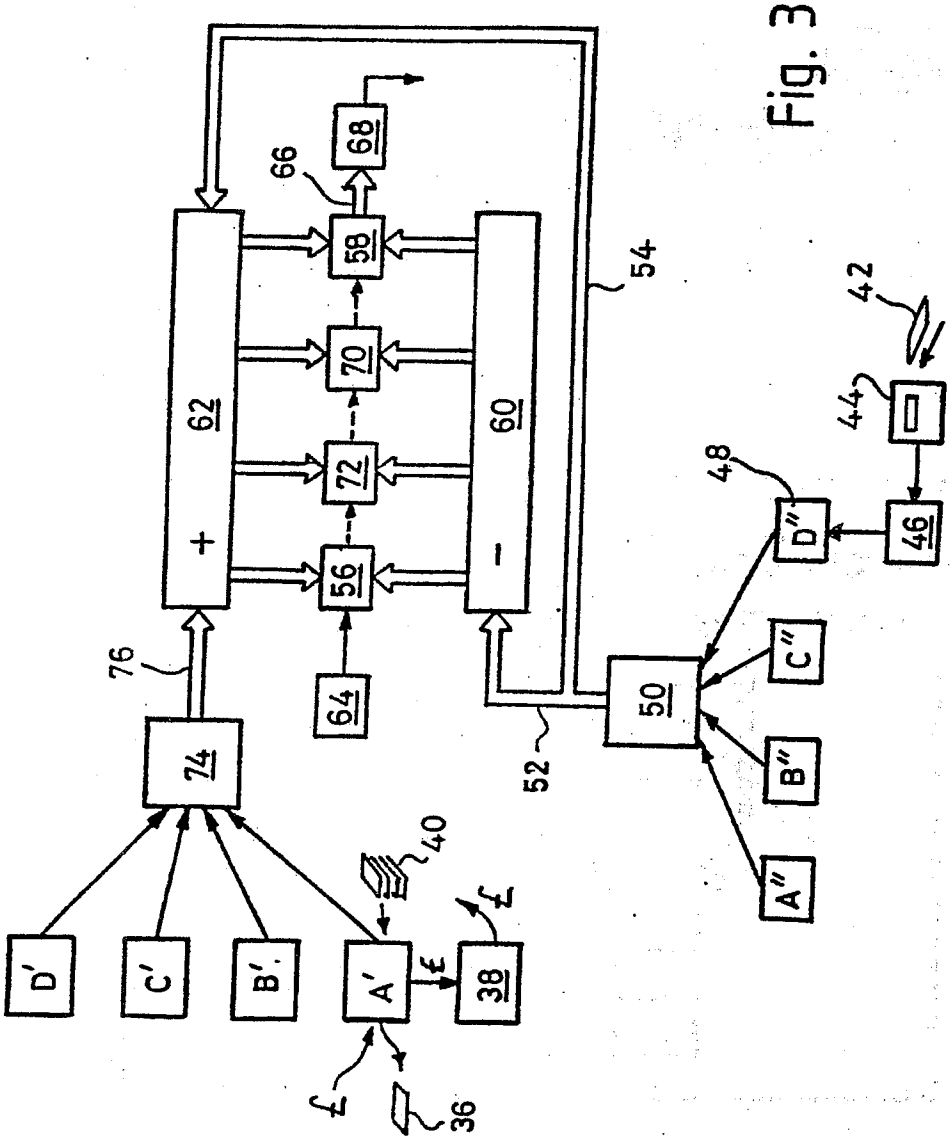

68
66
58
70
72
56
64
62
+
60
-
54
52
50
76
74
D'
C'
B'
A'
40
38
36
42
44
46
48
D"
C"
B"
A"

Fig. 3

INTERNATIONAL SEARCH REPORT

Interr al Application No
PCT/GB 95/00596

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/02 G07F9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F G07B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP,A,0 380 377 (URBA 2000) 1 August 1990 see abstract; claims; figures see column 8, line 28 - column 10, line 6	1-5
Y A	US,A,5 036 461 (J.C. ELLIOTT) 30 July 1991 see abstract; claim; figures see column 10, line 20 - column 11, line 25	1-5 6-13, 16-18, 22,30
A	US,A,4 758 954 (K. TAKIGUCHI) 19 July 1988	
A	EP,A,0 348 932 (OKI ELECTRIC INDUSTRY) 3 January 1990	
A	FR,A,2 605 770 (CGA-HBS) 29 April 1988	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 July 1995	03. 08. 95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/GB 95/00596

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,4 611 205 (D. EGLISE) 9 September 1986	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern al Application No
PCT/GB 95/00596

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0380377	01-08-90	FR-A-	2642202	27-07-90
		AT-T-	112876	15-10-94
		AU-A-	4871790	02-08-90
		CA-A-	2007335	25-07-90
		DE-D-	69013180	17-11-94
		DE-T-	69013180	24-05-95
		ES-T-	2066159	01-03-95
		JP-A-	2282862	20-11-90
		JP-B-	6022032	23-03-94
US-A-5036461	30-07-91	NONE		
US-A-4758954	19-07-88	NONE		
EP-A-0348932	03-01-90	JP-A-	2008984	12-01-90
		AU-B-	607339	28-02-91
		AU-A-	3710289	17-05-90
		DE-D-	68922531	14-06-95
FR-A-2605770	29-04-88	NONE		
US-A-4611205	09-09-86	AU-B-	569850	25-02-88
		AU-A-	2027083	03-05-84
		DE-A-	3375240	11-02-88
		EP-A,B	0109758	30-05-84
		GB-A,B	2129173	10-05-84
		GB-A,B	2172720	24-09-86
		JP-B-	7013824	15-02-95
		JP-A-	59121468	13-07-84

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04M 11/00, G07F 7/08 — A1

(11) International Publication Number: WO 96/41462

(43) International Publication Date: 19 December 1996 (19.12.96)

(21) International Application Number: PCT/US96/09785

(22) International Filing Date: 7 June 1996 (07.06.96)

(30) Priority Data:
08/487,813 7 June 1995 (07.06.95) US

(71) Applicant: ELECTRONIC DATA SYSTEMS CORPORATION [US/US]; 5400 Legacy Drive, M/S H3-3A-05, Plano, TX 75024 (US).

(72) Inventor: DENTILINGER, Dale, H.; 2105 Countryside Circle, Naperville, IL 60565 (US).

(74) Agent: GRIEBENOW, L., Joy; Electronic Data Systems Corporation, 5400 Legacy Drive, M/S H3-3A-05, Plano, TX 75024 (US).

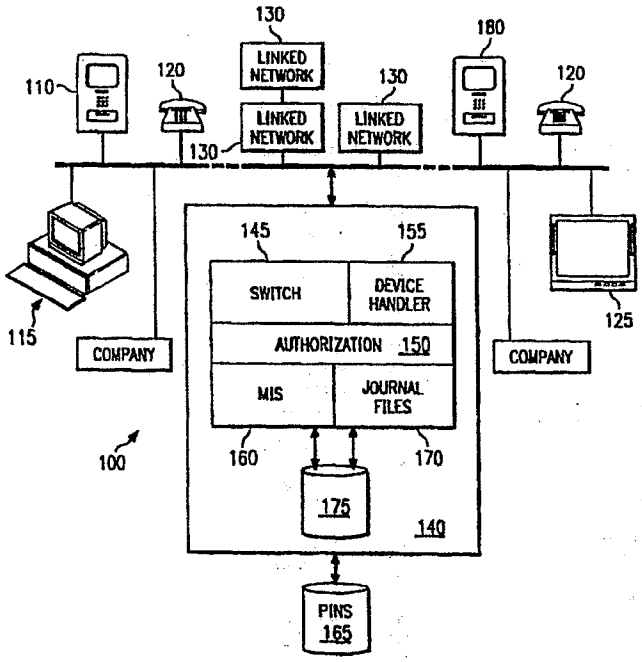
(81) Designated States: AU, BR, CA, JP, MX, NZ, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SYSTEM AND METHOD FOR DISPENSING OF A RECEIPT REFLECTING PREPAID PHONE SERVICES

(57) Abstract

A system and method for electronic purchase of prepaid telephone services is provided. An initiating terminal (110) receives input of a customer's request to purchase a specified amount of prepaid telephone services and receives input of the customer's designation of a financial account from which to electronically debit the price of such purchase. A central terminal (140) receives these inputs from the initiating terminal, obtains authorization for the request, and transmits data to the initiating terminal for the initiating terminal to, in turn, print on a receipt and provide to the customer. This receipt is then used instead of a telephone card to obtain telephone services up to the specified amount. Such receipt may also detail instructions and an authorization number, such as a personal identification number or PIN, to initiate the prepaid telephone service. The system and method of the present invention also preferably transfers the funds from the appropriate demand or credit account to pay for the purchased telephone services. An additional, separate Regulation E-type receipt is preferably also printed reflecting the financial transaction.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia
AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

SYSTEM AND METHOD FOR DISPENSING OF A RECEIPT REFLECTING PREPAID PHONE SERVICES

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates generally to prepaid phone services, and more particularly to a system and method for electronic dispensing of a receipt reflecting prepaid telephone services to be used by customers in place of current prepaid telephone cards, including electronic debiting of an account for costs associated therewith.

Description of the Related Art

Telephone companies currently sell a physical card product that allows consumers to purchase pre-paid phone services, such as long distance time, in predetermined increments of time, on the respective company's network(s). Consumers purchase these cards for the convenience of a calling card with the security of a pre-set spending limit. These cards may be the typical plastic cards normally associated with the debit and credit industry or are wallet-sized cardboard cards imprinted with PIN (personal identification number) information and dialing instructions. These cards are designed to be discarded once the time purchased is consumed. The value of the card is maintained on the respective telephone company's network system. For purposes of convenience, "Company" will refer hereinafter to the specific telephone system carrier on whose network time is to be pre-purchased.

Such prepaid telephone cards are sold at retail outlets, either over-the-counter or through vending machines. An ordinary retail receipt is issued for the cards purchased when the cards are purchased over-the-counter. Such receipts give the customer no additional

information other than that phone cards were purchased, the cost of the card(s) purchased, the date, and, normally, the retailer where the cards were purchased.

There are a number of drawbacks to the process described above. A customer must find a retail outlet which is open and is not out of calling cards. If a large purchase of telephone network time is desired, many retail outlets in the evening and night do not accept large denomination currency to pay for purchases. Additionally, the retail outlet must maintain and track a secured inventory of cards by number and denomination, and report the sales and number of cards sold to the Company. Such a system is very labor-intensive and costly to operate. Moreover, there is considerable expense on behalf of the Company to produce and distribute the cards to the retailers.

SUMMARY OF THE INVENTION

In view of the above problems associated with the related art, it is an object of the present invention to provide a system and method for dispensing a printed receipt which reflects prepaid phone services to be used by a customer instead of a telephone card.

It is another object of the present invention to provide a system and method for electronically dispensing such receipt via an automatic teller machine ("ATM") or personal computer fitted with a printer.

It is a further object of the present invention to provide a system and method for electronically debiting a designated account for the costs of the prepaid phone services reflected on such printed receipt.

The present invention achieves these and other objects by providing a system and method for electronically dispensing a receipt reflecting prepaid phone services from an initiating terminal, such as an Automated Teller Machine (ATM) or personal computer,

including electronic debiting of an account for costs associated therewith.

In one aspect of the present, a system and method for purchase of prepaid telephone services is provided. An initiating terminal receives input of a customer's request to purchase a specified amount of prepaid telephone services and receives input of the customer's designation of a financial account from which to electronically debit the price of such purchase. A central terminal receives these inputs from the initiating terminal, obtains authorization for the request, and transmits data to the initiating terminal for the initiating terminal to, in turn, print on a receipt and provide to the customer. This receipt is then used instead of a telephone card to obtain telephone services up to the specified amount. Such receipt may also detail instructions and an authorization number, such as a personal identification number or PIN, to initiate the pre-paid telephone service. The system and method of the present invention also preferably transfers the funds from the appropriate demand or credit account to pay for the purchased telephone services. An additional, separate Regulation E-type receipt is preferably also printed reflecting the financial transaction.

One advantage of the system and method of the present invention is that it allows a wider range of payment mechanisms for financing the transaction (e.g., credit, debit or smart cards). Many retail outlets at which traditional cards are sold do not take credit cards or debit cards. This limits the customer to paying with cash or check. Another advantage, when the initiating terminal is an ATM, is the convenience of purchasing prepaid telephone cards while a customer does their banking.

These and other features and advantages of the invention will be apparent to those skilled in the art

from the following detailed description of preferred embodiments, taken together with the accompanying drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic overview diagram illustrating an example network containing an embodiment of the present invention;

FIG. 2 is an illustrative example of a receipt printed by the system of the present invention;

FIG. 3 is a schematic illustration of principal and fee transfer according to a preferred embodiment of the present invention; and

FIG. 4 is a flowchart illustrating an embodiment of the method of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention electronically dispenses a receipt for prepaid telephone services to be used by customers in place of current prepaid telephone cards. As a brief overview, a customer desiring to purchase prepaid telephone services preferably uses an ATM to access the system services of the present invention. It should be understood that the customer could instead have used a personal computer outfitted with the capability to access the system service of the present invention and a printer. With either option (ATM or personal computer), the customer preferably interacts with the system of the present invention via a graphic user interface (GUI).

Regardless of the input terminal selected (personal computer, ATM, etc.), the customer preferably uses a card to make funds available from a financial account corresponding to the card. Such card could be a credit card, debit card, smart card or stored value card. At this point, the funds to be transferred are held or pre-authorized as available and the customer's account is debited. A customer's account may also be debited the amount of a customary transaction or convenience fee. A convenience fee may be charged for each prepaid telephone service transaction. At least one receipt is printed for the customer showing an "800 number", a PIN, and how much time has been purchased. An example of how such a receipt 200 might appear is illustrated in FIG. 2 and discussed in more detail below. The customer calls the "800" number, enters the PIN number, and preferably hears a recording telling the customer that he has a predetermined amount of time to talk, depending on how much time he purchased. By following the Company's recorded prompts, the customer then dials the destination telephone number he wanted to call and begins talking. As there are many ways to carry out customer interaction with a Company, and such is beyond the scope of the present invention, it will not be described in further detail.

The present invention can probably best be understood by considering it as two distinct transactions, which will hereinafter be referred to as "requesting" and "dispensing", together comprising the overall transaction. Those of ordinary skill in the art will understand considering the initiating terminal as an "issuer" and the central terminal as an "acquirer" for purposes of the requesting transaction, as well as considering the central terminal as an "issuer" and the initiating terminal as an "acquirer" for purposes of the dispensing transaction. The requesting transaction is preferably portrayed as a withdrawal, or a withdrawal with a convenience charge, as may be the case.

The requesting transaction may be logically considered to include a request to purchase prepaid telephone services, a request for authorization, and an approval (if any). Consider FIG. 1, which is a schematic diagram of an example network illustrating an embodiment of the present invention. The requesting portion of the overall transaction begins with a request to electronically purchase prepaid telephone services from an initiating terminal. This "terminal" is the medium a customer uses to create the request to electronically purchase the prepaid telephone services, e.g., ATM 110, personal computer 115 with a Graphical User Interface (GUI), etc. The GUI preferably supports at least Windows, DOS or Macintosh environments. For the sake of the following discussion, and unless otherwise stated, initiating terminal 110 will be an ATM. It should be understood that any of the initiating terminals ATM 110, personal computer 115, screen telephone with printing mechanism 120, or television with printing mechanism 125 could have been used instead. Moreover, initiating terminal 110 may be physically situated anywhere including a convenience store, a grocery store, a post office, a branch of a financial institution, a mall, or other location.

Initiating terminal 110 preferably permits the transmission of debit or credit card information with the associated PIN encrypted and encoded to ensure security as to the debit or credit card information. Such terminal, if not an ATM which is customarily DES-secure, preferably includes a device (not shown) attached to the communications line which securely encrypts information. Several companies manufacture a device which securely encrypts information, such as ised corporation, and therefore such device will not be described in further detail herein.

As noted above, the requesting portion of the overall transaction according to the present invention begins with a customer's request to electronically purchase prepaid telephone services from initiating terminal 110. The screen or menu will have the normal transaction options: withdrawal, balance inquiry, deposit, etc. However, with the present invention, a customer can now also purchase pre-paid telephone services by selecting the transaction option to purchase such services. The transaction to purchase prepaid telephone services may be offered in a selection menu as "Company Prepaid Telephone Card", as an example. The customer selects the appropriate option from the screen or menu by pressing a button or touching a screen, depending upon the initiating terminal 110, to interact with system 100 of the present invention. If the customer chooses the prepaid telephone services option, initiating terminal 110 preferably requests, via at least one screen or additional prompt, certain information from the customer, such as what denomination of prepaid telephone services are desired to be purchased, and then, the financial account from which such purchase is to be electronically debited. The customer is also informed of any convenience fee to be assessed, if any, to perform the desired transaction.

Normally, the customer has already inserted a card to activate ATM 110. ATM 110 of the present invention preferably assumes that the card corresponds to the financial institution from which the customer will pay for the purchase. ATM 110 preferably inquires whether the customer wishes to have the funds taken from the customer's checking account, savings account, etc. The customer makes the desired selection. System 100 transmits the request to purchase prepaid telephone services, together with the financial account from which the customer desires to have funds electronically withdrawn to pay for such purchase, to central terminal 140.

It should be understood that initiating terminal 110 could instead have prompted the customer to designate the account to be debited the costs of the transaction before offering the customer a screen showing the dollar amounts from which to choose. For the sake of discussion, it will be assumed that the dollar amounts of prepaid telephone services are fixed, and are in the amounts of $10, $20 and $50. It will be appreciated that such amounts are for illustration purposes only, and in no way should be construed to limit the scope of the present invention.

Initiating terminal 110 then preferably builds a Point of Sale ("POS") transaction and passes the POS transaction to modular device handler 155. Device handler 155 builds a standard transaction message based on the contents of POS transaction received from initiating terminal 110 and sends the transaction message to router/switch 145. The standard transaction message fields are preferably filled as follows:

- Type - "0200"
- Transaction type - "44xx00"
  [indicating a purchase of goods or services from "xx", where "xx" is the account type.]
- Point of Service ("POS") condition code - "14"

[indicating a generic point of sale]

- Merchant ID - "Company"
  [where "Company" is the actual name of the telephone service provider of the services for which the customer wishes to prepay]
- Initiating Terminal Dispense Type -
  "7" $10 worth of prepaid telephone services dispensed
  "8" $20 worth of prepaid telephone services dispensed
  "9" $50 worth of prepaid telephone services dispensed
- Merchant Type - "4812"
  [indicating that the telephone service/equipment is non-utility, non-regulated]
- POS Data Code - "22140121010C"
  [Card data input capability "2" - magnetic stripe read
  Cardholder authentication "2" - PIN
  Card Retention capability "1" - can capture
  Operating environment "4" - off premises of terminal owner, unattended
  Cardholder present "0" - cardholder present
  Card present "1" - card present
  Card data input mode "2" - magnetic stripe read
  Cardholder authentication "0" - non-authenticated
  Cardholder authentication mode "1" - PIN
  Security data "0" - no security concern
  Pin capture capability "C" - 12 characters]
- Service Classification Code - "700"
  [indicating this transaction is a general purchase of services]

By employing the standard transaction message populated as described above, initiating terminal 110 preferably

transmits the requested transaction information received from the customer by a high-speed dedicated line to central terminal 140.

Initiating terminal 110 determines that the subject transaction requires authorization and sends a request for authorization to central terminal 140, thereby entering the next stage of the requesting transaction. While various implementations will occur to those skilled in the art, central terminal 140 preferably includes switch 145, authorization unit 150, suspended journal files 170, and modular device handler 155 running on a Tandem-based platform for real-time processing, a SUN 2000 workstation for relational database 175 and MIS journal files 160, and an ESA9000 IBM mainframe for off-line (batch) processing, financial records maintenance, research, and reporting. Some of the many types of reports include: reconciliation of sold and unsold PINs, account of number of receipts 200 by denomination, summary of total PINs sold, etc. PINs 165 contains the different denominations of prepaid phone services that Company desires to sell ($10, $20 and $50 for purposes of the present discussion). The PIN numbers in PINs file 165 are preferably live and encrypted.

Switch 145 of central terminal 140 accepts the incoming request and activates authorization unit 150. Authorization unit 150 in turn forwards the request to an authorization agent (not shown). Central terminal 140 preferably has the appropriate linkages to debit card networks and credit card authorization points to authenticate the card and the account information belonging to the customer desiring to make the purchase. Among the information provided to the authorization agent is the request for authorization for the principal amount corresponding to the desired level of prepaid telephone services selected by the customer (referred herein as "the principal"), together with the appropriate convenience or service fee, if any.

The authorization agent receives the financial information from central terminal 140 and, assuming sufficient funds or credit exists in the referenced account, authorizes the transaction for the full amount of the principal and any convenience fee. It should be understood that the authorization agent may be a financial institution, a card issuer, an intercept processor, or a regional/national network. The system of the present invention permits customization to thereby allow the participating institutions to set their own approval limits for their customers.

As there are numerous known ways for obtaining authorization, any of which are compatible with the system and method of the present invention, the actual authorization method carried out by an authorization agent will not be considered in more detail herein. Moreover, it should be understood that the platform of central terminal 140 of the present invention may also be the authorization agent and perform authorization approval with the permission and within the guidelines established by a particular financial institution.

Once the authorization agent returns an approval message to central terminal 140, the requesting transaction has entered the authorization-approved stage. When central terminal 140 receives an approved transaction response, central terminal 140 writes an entry to journal files 170 and logs the transaction in relational databases 175 for long-term storage, retrieval, and reporting for subsequent research on that data. This entry should correctly represent the transaction, but is not included in any dollar-dispensed totals accrued to the ATM. If the customer selected $50 of prepaid services, and an approval is returned from the authorization agent, the transaction is preferably processed as a POS transaction for $50, i.e., for the dispense of one $50 prepaid telephone services receipt 200. The ATS screen and balancing receipt is preferably

modified to included counts of telephone receipts 300 dispensed, by denomination. However, it is preferred that no change be made to the standard Regulation E financial transaction receipt.

Return momentarily to FIG. 2 which illustrates an example receipt 200 for prepaid telephone services. The key components are the clear, live PIN, the Company number to call to access the services paid for (preferably toll-free), and any expiration date of the PIN. These elements are taken directly from the TENS, TWENTIES and FIFTIES files, except for the clear PIN. Device handler 155 decrypts the KPE using variant zero of the "known" KKE, then decrypts the PIN using variant zero of the clear KPE.

Receipt 200 is preferably printed prior to printing the financial transaction receipt. If the receipt printer faults before receipt 200 is completely printed, initiating terminal 110 preferably reverses the transaction. Initiating terminal 110 will then immediately report a receipt printer fault and the transaction menu item "Prepaid telephone services" will not be available. If a reversal occurs, regardless of reason, device handler 155 preferably returns the entire record - the encrypted PIN, encrypted KPE, toll-free #, batch number, expiration date and file key to central terminal 140 for insertion back into the appropriate TENS, TWENTIES or FIFTIES file in PINs database 165.

The second portion of the overall transaction, the dispensing transaction, will now be considered. When the transaction response is returned by authorization 150 to device handler 155 as approved, device handler 155 formats a request to central terminal 140 for the next available PIN in the appropriate TENS, TWENTIES or FIFTIES files. It should be observed at this point that if the transaction is returned by the authorization agent as not approved, device handler 155 delivers the denial to initiating terminal 110 for communication to the

customer, without requesting a PIN from central terminal 140.

Central terminal 140 returns to device handler 155 a message containing the PIN, the associated KPE, a toll-free number, batch number, and the file key. Central terminal 140 deletes the record from the TENS, TWENTIES, OR FIFTIES file of PINs 165 at this time. Device handler 155 transmits the PIN to initiating terminal 110, which in turn prints the PIN on issued receipt 200 for the customer. The PIN can be provided to the customer via a variety of methods, depending upon initiating terminal limitations, but preferably it is provided to the customer on receipt 200. Initiating terminal 110 preferably also issues a separate receipt (standard Regulation E) which itemizes the principal amount transferred to pay for the phone services purchased, and the convenience fee charged the customer's account for the transaction, if any, and from which account such funds were electronically debited. It should be understood that while two separate receipts may be issued by initiating terminal 110, according to another embodiment of the present invention, initiating terminal 110 issues only one receipt bearing on its face all of the information found on the two separate receipts of the preferred embodiment.

It should be understood by those skilled in the art that central terminal 140 of the present invention may be accessed, preferably via high-speed dedicated lines, from any number of networks 130 with their own initiating terminals and financial institutions with which they are associated. Because of this open design, an initiating terminal 110, such as an ATM, on a different network 130 than central terminal 140 may obtain authorization for and receive a live PIN to be provided to their customer.

Company is preferably connected to central terminal 140 by dial-up transmission line, but it will be understood that a dedicated line could be used instead.

It should also be understood that more than one Company may be supported by the present system, in which case separate PINs 165 could be maintained for each Company supported.

As needed, new live PINs are provided by Company in a file called PINFILE to replenish PINs 165. PINFILE's record length is 80 bytes. Example file and record layouts for PINFILE are contained in Table A. The file is usually transmitted using an RJE SNA protocol dialup connection (remote 241) to central terminal 140. Each PIN number is preferably associated with a set amount of telephone service time corresponding to a given denomination shown in receipt 200. Thus, when Company's system encounters a PIN number, it knows that the encountered PIN number is a $20 PIN number, for example, and accordingly responds.

TABLE A - PINFILE

PINFILE file header:

Element	Description	Attribute	
Record Type	"H"	1	A
File Replacement Code	"L" or "U"	1	A
File Name	"PINFILE"	7	A
Filler	blank	65	S
Record Number	"000001"	6	N

PINFILE detail record:

Element	Description	Attribute	
Record Type	"D"	1	A
PIN	hex character set, 0-F	16	AN
Filler	blank	1	S
KPE	hex character set, 0-F	16	AN
Filler	blank	1	S
Denomination	"10" or "20" or "50"	2	AN
Filler	blank	1	S
Denomination	"10" or "20" or "50"	2	AN
Filler	blank	1	S
800#	character set, 0-9	7	N
	This is the 800 number the consumer calls - printed on receipt 200		
Filler	blank	1	S
Expiration date	MMDDYYYY	8	N
Filler	blank	1	S
Batch #	Comp. batch number, right justified, zero filled	9	N
	printed on receipt 200		
Filler	blank	10	S
Record Number	sequential within file, right justified, zero filled	6	N

PINFILE trailer record:

Element	Description	Attribute	
Record Type	"T"	1	A
Total Number of $10 Records	count of $10 PINs detail records	6	N
Total Number of $20 Records	count of $20 PINs detail records	6	N
Total Number of $50 Records	count of $50 PINs detail records	6	N
Total Dollars	total $ for all detail records	6	N
Total Record	record count in file, including header and trailer records	7	N
Filler	blank	42	S
Records Number	sequential within file, right justified, 0 filled	6	N

Explanation of terms for Table A:

Batch # - The Company batch from which the particular PIN has been taken. This number will be printed on receipt 200.

Denomination - "10" or "20" or "50" (i.e., the dollar amount associated with the PIN).

File Replacement Code - "L" indicates a full file load and "U" indicates an update. A full file load should only be performed for the first file sent. All files subsequent to the first file should be updates.

Expiration Date - Preferably assigned by Company, sent in MMDDYYYY format. Will be printed on receipt 200.

File Name - Constant "PINFILE".

PIN - The encrypted PIN. This is a 16-character hex number resulting when the 10 character clear PIN is encrypted under a Key for PIN Encryption (KPE).

KPE - The encrypted Key for PIN Encryption. This is the key used for encrypting the PIN, encrypted under a Key for Key Encryption (KKE).

Record Number - A sequential number, incremented by 1, associated with the record in the file. The header record should always be "000001".

Record Type - Constant "H" for a header record, constant "D" for detail records, or constant "T" for a trailer record.

Total Dollars Represented - Total dollars represented by all detail records.

Total Number of $10 Records - Count of detail records containing $10 PINs.

Total Number of $20 Records - Count of detail records containing $20 PINs.

Total Number of $50 Records - Count of detail records containing $50 PINs.

Total Records - Count of all records in file, including header and trailer records.

800# - This is the last seven digits of the toll-free number a consumer will call to use the prepaid telephone services reflected by his receipt 200. This number, formatted "800-NNN-NNNN" will be printed on receipt 200.

Central terminal 140 builds three key-sequenced files for storage of the new PINs in PINS 165, one for each denomination of prepaid telephone services available for purchase: $10, $20, or $50. Each record preferably consists of the encrypted PIN, the key under which the PIN has been encrypted, the expiration date associated with the PIN, the Company batch number from which the PIN has been taken, and the last seven digits of the toll-free number associated with this PIN. The Key for PIN Encryption (KPE) is stored encrypted under a Key for Key Encryption (KEK). While the KEK is preferably generated by the Company, central terminal 140 can also be adapted to generate the KEK. The KEK value is input as a run-time parameter to device handler 155, which, as was mentioned earlier, is responsible for the decryption of each PIN as it is removed from PINs 165 and transmitted to the customer.

Consider momentarily FIG. 3, which is a schematic block illustration of principal and fee (if any) transfer according to a preferred embodiment of the present invention. Upon receipt of the approval message, which amounts to approval of the authorization request and reflects the fact the customer does in fact have sufficient funds available, central terminal 140 "withdraws" the money from the customer's account 310 and credits holding account 320. Central terminal 140 also credits holding account 340 with a convenience fee, if any. The transaction is normally settled on a predetermined basis among the parties owning the pieces of the system responsible for carrying out the overall transaction. The distribution of the settlement is preferably a batch process.

As is the normal business practice within the electronic funds transfer (EFT) industry, once system 100 of the present invention has received an authorization approval message, the relevant financial institution has committed to reimburse the owner of initiating terminal

110 (an ATM in the present example) that will, in effect, be advancing funds on the customer's behalf when initiating terminal 110 dispenses receipt 200 for prepaid telephone services to the customer. Thus, the authorization approval is a guarantee on the part of the issuing institution that the acquiring institution will be reimbursed. For this reason, system 100 of the present invention can complete the overall transaction even in advance of actually getting the funds from the institution.

Consider lastly FIG. 4, which is a flowchart illustrating an embodiment of the method of the present invention. At Block 410 initiating terminal 110 receives a request to purchase a specified amount of prepaid telephone services (as described hereinabove) from a customer. Initiating terminal 110 requests and receives input from the customer designating a financial account from which central terminal 140 is to electronically debit the price of such purchase (block 420). Central terminal 140 requests authorization for such purchase from the authorizing agent responsible for the financial account designated by the customer at block 430. Assuming authorization is obtained, central terminal 140 then journals the transaction (block 440). Central terminal 140 may at this point electronically debit the specified financial account (block 450). Next, central terminal 140 obtains a PIN from PINs 165. This PIN is transmitted, at block 460, to initiating terminal 110, together with whatever calling instructions Company designates. It should be understood that the calling instructions to be printed on the receipt may be stored at initiating terminal 110 instead of being transmitted from central terminal 140. Initiating terminal 110 then prints a receipt (block 470), which is provided to the customer. This receipt contains the transmitted PIN and instructions, and is used instead of a telephone card to obtain telephone services up to the specified (purchased)

amount. At block 480 a separate Regulation E-type receipt is preferably also printed.

It should be understood by those skilled in the art that the present description is provided only by way of illustrative example and should in no manner be construed to limit the invention as described herein. Numerous modifications and alternate embodiments of the invention will occur to those skilled in the art. Accordingly, it is intended that the invention be limited only in terms of the following claims:

WE CLAIM:

1. A system for purchase of prepaid telephone services, comprising:

an initiating terminal for receiving input of a customer's request to purchase a specified amount of prepaid telephone services, and receiving input of said customer's designation of a financial account from which to electronically debit the price of such purchases; and

a central terminal receiving said inputs from said initiating terminal, obtaining authorization for said request, and transmitting data to said initiating terminal for said initiating terminal to print on a receipt and provided to said customer, which receipt may be used instead of a telephone card to obtain telephone services up to said specified amount.

2. The system for purchase of prepaid telephone services of Claim 1, wherein said central terminal electronically debits said financial account before transmitting said data to said initiating terminal.

3. The system for purchase of prepaid telephone services of Claim 1, wherein said initiating terminal is an automated teller machine (ATM).

4. The system for purchase of prepaid telephone services of Claim 1, wherein said initiating terminal is a personal computer with a graphical user interface.

5. The system for purchase of prepaid telephone services of Claim 1, wherein said central terminal journals said transaction after obtaining authorization for said request.

6. The system for purchase of prepaid telephone services of Claim 1, wherein said data transmitted by said central terminal to said initiating terminal includes a personal identification number (PIN).

7. The system for purchase of prepaid telephone services of Claim 1, wherein said data transmitted by said central terminal to said initiating terminal includes instructions to access said prepaid telephone services.

8. The system for purchase of prepaid telephone services of Claim 1, wherein said initiating terminal also prints a separate Regulation E-type receipt.

9. The system for purchase of prepaid telephone services of Claim 1, wherein said initiating terminal also includes a financial card reader.

10. A method for automated purchase of prepaid phone services, comprising the steps of:

receiving, at an initiating terminal, input of a request to purchase a specified amount of prepaid telephone services;

obtaining financial authorization for said request by a central terminal;

printing of a receipt reflecting purchase of prepaid phone services to be used instead of a telephone card to obtain telephone services up to said specified amount.

11. The method for automated purchase of prepaid phone services of Claim 10, further comprising the step of electronically debiting a financial account for the price of such purchase before said step of printing of a receipt.

12. The method for automated purchase of prepaid phone services of Claim 11, wherein said step of receiving input further comprises the step for receiving input of a designation of a specified financial account from which to electronically debit the price of such purchase.

13. The method for automated purchase of prepaid phone services of Claim 10, wherein said step of printing a receipt further comprises the step for printing instructions on accessing said prepaid telephone services.

14. The method for automated purchase of prepaid phone services of Claim 10, further comprising the step of printing an additional separate Regulation E-type receipt.

15. The method for automated dispensing of a receipt reflecting purchase of prepaid phone services of Claim 10, wherein said initiating terminal is an automated teller machine (ATM).

16. The method for automated dispensing of a receipt reflecting purchase of prepaid phone services of Claim 10, wherein said initiating terminal is a personal computer with a graphical user interface.

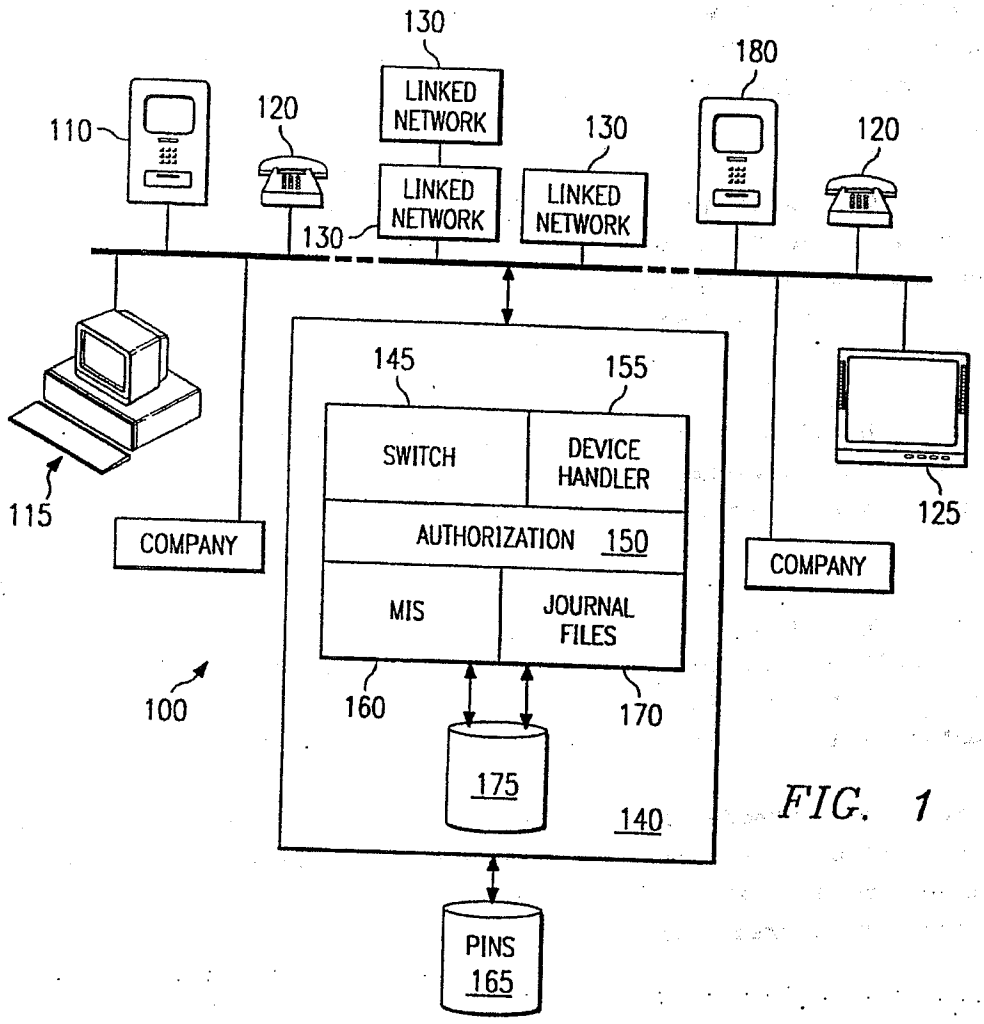
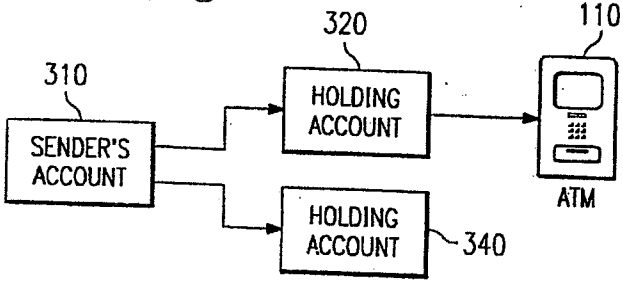

130
LINKED NETWORK
180
110
120
LINKED NETWORK
130
LINKED NETWORK
120
130
145
155
SWITCH
DEVICE HANDLER
AUTHORIZATION 150
MIS
JOURNAL FILES
115
COMPANY
COMPANY
125
100
160
170
175
140
PINS 165

FIG. 1

FIG. 3


320
110
310
HOLDING ACCOUNT
SENDER'S ACCOUNT
ATM
HOLDING ACCOUNT
340

200

FIG. 2

COMPANY

Telephone Card

You have purchased

$ XXXX

of prepaid calling.

- TO PLACE CALLS:

  1. Dial 1-XXX-XXX-XXXX from any touchtone phone.
  2. At prompt, enter XXX-XXX-XXXX
  3. Follow prompts to place calls

- NEXT CALL - DON'T HANG UP!

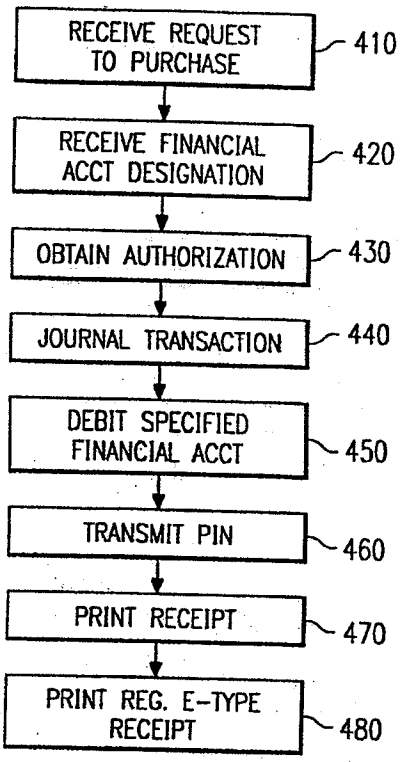
  Push # for one full second and follow prompts for next call.

- CALL 1-XXX-XXX-XXXX FOR 24 HOUR CUSTOMER SERVICE

BATCH XXXXXX EXPIRES XX/XX/XX

No cash redemptive value. Cannot be applied to any Company invoice. Non-refundable. Non-transferrable.

FIG. 4



INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 96/09785

A. CLASSIFICATION OF SUBJECT MATTER

H 04 M 11/00,G 07 F 7/08

According to International Patent Classification (IPC) or to both national classification and IPC 6

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H 04 M,G 07 F,H 04 Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 5 352 876 (WATANABE et al.) 04 October 1994 (04.10.94), abstract; column 1, line 10 - column 2, line 19; fig. 1; claims 1,8,12,13. --	1,10
A	EP, A, 0 380 434 (SOCIETE DE FABRICATION D'APPAREILS AUTOMATIQUES ET DE SIROPS) 01 August 1990 (01.08.90), abstract; column 1, lines 1-30; fig. 1; claims 1-3. --	1,10
A	US, A, 5 146 067 (SLOAN et al.) 08 September 1992 (08.09.92),	1,10

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 October 1996	12.11.96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer BADICS e.h.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 96/09785

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	abstract; column 1, line 6 - column 2, line 69; fig. 1; claims 1,3,4. ----	

ANHANG

zum internationalen Recherchenbericht über die internationale Patentanmeldung Nr.

ANNEX

to the International Search Report to the International Patent Application No.

ANNEXE

au rapport de recherche international relatif à la demande de brevet international n°

PCT/US 96/09785 SAE 136996

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten internationalen Recherchenbericht angeführten Patentdokumente angegeben. Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The Office is in no way liable for these particulars which are given merely for the purpose of information.

La présénte annexe indique les membres de la famille de brevets relatifs aux documents de brevets cités dans le rapport de recherche international visée ci-dessus. Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsibilité de l'Office.

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
US A 5352876	04-10-94	JP A2 4209085	30-07-92
EP A1 380434	01-08-90	CA AA 2007871	17-07-90
		FR A1 2641886	20-07-90
US A 5146067	08-09-92	AU A1 66822/90	18-07-91
		AU B2 636181	22-04-93
		NZ A 236202	26-01-94
		WO A1 9110976	25-07-91